

DHS'S PROGRESS IN SECURING ELECTION SYSTEMS AND OTHER CRITICAL INFRASTRUCTURE

HEARING BEFORE THE COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JULY 11, 2018

Serial No. 115-70

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

33-942 PDF

WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas	BENNIE G. THOMPSON, Mississippi
PETER T. KING, New York	SHEILA JACKSON LEE, Texas
MIKE ROGERS, Alabama	JAMES R. LANGEVIN, Rhode Island
LOU BARLETTA, Pennsylvania	CEDRIC L. RICHMOND, Louisiana
SCOTT PERRY, Pennsylvania	WILLIAM R. KEATING, Massachusetts
JOHN KATKO, New York	DONALD M. PAYNE, JR., New Jersey
WILL HURD, Texas	FILEMON VELA, Texas
MARTHA MCSALLY, Arizona	BONNIE WATSON COLEMAN, New Jersey
JOHN RATCLIFFE, Texas	KATHLEEN M. RICE, New York
DANIEL M. DONOVAN, JR., New York	J. LUIS CORREA, California
MIKE GALLAGHER, Wisconsin	VAL BUTLER DEMINGS, Florida
CLAY HIGGINS, Louisiana	NANETTE DIAZ BARRAGÁN, California
THOMAS A. GARRETT, JR., Virginia	
BRIAN K. FITZPATRICK, Pennsylvania	
RON ESTES, Kansas	
DON BACON, Nebraska	
DEBBIE LESKO, Arizona	

BRENDAN P. SHIELDS, *Staff Director*
STEVEN S. GIAIER, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
HOPE GOINS, *Minority Staff Director*

CONTENTS

	Page
STATEMENTS	
The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Chairman, Committee on Homeland Security:	
Oral Statement	1
Prepared Statement	2
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Oral Statement	3
Prepared Statement	37
The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas:	
Prepared Statement	38
WITNESSES	
Mr. Christopher C. Krebs, Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security:	
Oral Statement	42
Prepared Statement	43
Ms. Nellie M. Gorbea, Secretary of State, State of Rhode Island:	
Oral Statement	49
Prepared Statement	51
FOR THE RECORD	
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Letters	5
Press Releases	23
Documents	33
APPENDIX	
Questions From Honorable John Katko for Christopher C. Krebs	89
Questions From Honorable John Ratcliffe for Christopher C. Krebs	90
Questions From Honorable James R. Langevin for Christopher C. Krebs	90

DHS'S PROGRESS IN SECURING ELECTION SYSTEMS AND OTHER CRITICAL INFRA- STRUCTURE

Wednesday, July 11, 2018

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to notice, at 10:31 a.m., in room HVC-210, Capitol Visitor Center, Hon. Michael T. McCaul (Chairman of the committee) presiding.

Present: Representatives McCaul, King, Rogers, Barletta, Perry, Katko, Hurd, McSally, Fitzpatrick, Estes, Bacon, Lesko, Thompson, Jackson Lee, Langevin, Keating, Payne, Vela, Watson Coleman, Rice, Correa, Demings, and Barragán.

Chairman McCaul. The Committee on Homeland Security will come to order.

The committee is meeting today to examine the work that the Department of Homeland Security is doing to assist State and local officials to secure election infrastructure, including voting machines, vote tallying systems, and voter databases.

In addition to election security, we will also examine DHS's role working across all 16 critical infrastructures, because a cyber threat to elections may pose a similar threat to other critical infrastructure sectors.

I now recognize myself for an opening statement.

Our democratic system and critical infrastructures are under attack. In 2016, Russia meddled in our Presidential election through a series of cyber attacks and information warfare. Their goals were to undermine the credibility of the outcome and sow discord and chaos among the American people.

This was a provocative attack against our country; we must not allow it to happen again. I have stated repeatedly and long before the last election that foreign interference in our democracy cannot be tolerated. I strongly believe we will be targeted again this November in the midterm elections, and we need to be prepared.

That is why we included \$380 million in grants to the Election Assistance Commission and \$26 million to the Department of Homeland Security for election infrastructure in fiscal year 2018. These funds will enhance election technology and bolster cyber readiness.

However, malicious use of the internet and the exploitation of social media are not just aimed at our election systems. In March, the FBI and DHS reported that Russian hackers attacked Amer-

ican nuclear power plants. Crippling or shutting down major parts of our energy sector would be catastrophic.

Russia has already done this to our allies. In 2015, a cyber attack turned off electricity for hundreds of thousands of Ukrainians. Last year, I stood on the front lines of Russia's cyber war in Ukraine and saw the effects first-hand.

Nation-state hacking is real and it is dangerous. Unfortunately, Russia is not the only villain. Between 2011 and 2013, Iranian hackers attacked dozens of U.S. banks and tried to shut down a dam in New York. In 2014, Chinese hackers stole 22 million security clearances from OPM, including my own. These attacks and others are part of a greater onslaught being waged against the United States.

As a result, I have made strengthening our cybersecurity a top priority of this committee. In the past year we have passed legislation to create the Cyber Security and Infrastructure Security Agency to elevate and operationalize the cybersecurity mission at DHS; authorize cyber incident response teams to assist local and State officials in identifying cyber risks and restoring essential services; and reauthorize DHS to ensure it offers services to local and State election officials upon request.

We are proud of these accomplishments, but we can always do more. So today's hearing gives us a chance to offer new ideas and promote new solutions to help protect our elections and other critical infrastructures.

I would like to thank the witnesses for being here today. We are grateful for your service to the country and expertise and look forward to working with each of you.

[The statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

JULY 11, 2018

Our democratic system and critical infrastructure are under attack.

In 2016, Russia meddled in our Presidential election through a series of cyber attacks and information warfare. Their goals were to undermine the credibility of the outcome and sow discord among the American people.

This was a provocative attack against our country and we must not allow it to happen again.

I have stated repeatedly, and long before the last election, that foreign interference in our democracy cannot be tolerated.

I strongly believe we'll be targeted again this November. We need to be prepared.

That is why we included \$380 million in grants to the Election Assistance Commission and \$26 million to DHS for election infrastructure in the fiscal year 2018 omnibus. These funds will enhance election technology and bolster cyber readiness.

However, malicious use of the internet and the exploitation of social media are not just aimed at our election systems.

In March, the FBI and DHS reported that Russian hackers attacked American nuclear power plants. Crippling or shutting down major parts of our energy sector would be a catastrophe.

Russia has already done this to our allies.

In 2015, a cyber attack turned off electricity for hundreds of thousands of Ukrainians.

Last year, I stood on the front lines of Russia's cyber war in Ukraine and saw the effects first-hand.

Nation-state hacking is real and dangerous. Unfortunately, Russia is not the only villain.

Between 2011 and 2013, Iranian hackers attacked dozens of U.S. banks and tried to shut down a dam in New York.

In 2014 Chinese hackers stole 22 million security clearances from OPM, including my own.

These attacks, and others, are part of a greater onslaught being waged against the United States.

As a result, I have made strengthening our cybersecurity a top priority of this committee.

In the past year we have passed legislation to:

- Create the Cybersecurity and Infrastructure Security Agency (CISA)—to elevate and operationalize the cybersecurity mission at DHS,
- Authorize Cyber Incident Response Teams—to assist local and State officials in identifying cyber risks and restoring essential services,
- Reauthorize DHS—to ensure DHS offers services to local and State election officials when requested (Richmond amendment).

We are proud of these accomplishments but we can always do more.

Today's hearing gives us a chance to offer new ideas and promote solutions to help protect our elections and other critical infrastructure.

I'd like to thank the witnesses for joining us today. This committee is very grateful for your service and expertise and we look forward to working with each of you.

Chairman MCCAUL. With that, the Chairman now recognizes the Ranking Member.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I want to thank you for holding today's hearing on election security.

I, too, would like to congratulate and thank Under Secretary Krebs for being here today. Good seeing you. I look forward to working with you to make sure DHS legislative authorities and responsibilities related to cybersecurity are well understood, and to ensure that the Department has the resources it needs to carry out the mission effectively.

Under Secretary, you have taken the job at a critical moment in our Nation. However, I am concerned you do not have the support you need from the White House.

You are responsible for building private-sector confidence in DHS information-sharing programs like Automated Indicator Sharing after President Trump toyed with the idea of planting an absurd story to discredit its own—for its own political purposes.

You are responsible for securing Federal networks at a time when the White House National security advisor has decided to eliminate the National Security Council's cybersecurity coordinator.

You are responsible for helping secure critical infrastructure networks for a White House that would rather save jobs in China than heed the advice of intelligence community on supply chain vulnerabilities.

And you are responsible for helping State and local governments secure election infrastructures following Russia's brazen election meddling efforts in 2016, which the President has been reluctant to call out and which Congressional Republicans, until recently, were content to ignore.

As we sit here today, President Trump is in Europe complicating your mission. Instead of working with our European allies to confront Russia, a shared adversary whose attempts to undermine Western Democratic institutions are growing more and more bold, he is trolling them to curry favor with Russian President Vladimir Putin.

President Trump has said he will address Russia's 2016 election meddling in a meeting with Putin, but he has never demonstrated a credible ability to confront Putin in our intelligence community's findings. He has predicted his meetings with Putin may be the

easiest, so I know and I have no reason to believe anything productive will come of it.

This President's failure to take seriously the threat to our democracy is one of the main reasons that we must do effective and thorough oversight in this body.

Although I am pleased that the Majority has finally scheduled today's hearing, I am disappointed that the Majority failed to invite a full range of stakeholders, including the Election Assistance Commission, or hold the hearing at a time when DHS's Federal partners were available to participate.

It is important to note for the record that committee Democrats have been requesting official oversight activities on elections security since before the 2016 election.

In March 2017, after months of inaction by the Republican majority, I introduced a resolution of inquiry seeking information from the Department on its activities relating to counter—countering Russian election interference in the 2016 Presidential election, so we would understand how to protect our elections in the future. It was unceremoniously rejected along party lines.

Committee Democrats have written to the Chairman no less than 5 times since August 2016 to request a hearing, briefing, or investigation on vulnerabilities to our election infrastructure. We have also reiterated these requests on numerous occasions on the record.

Despite these repeated requests, this committee did not conduct a formal hearing or briefing on the topic until April 2018, 15 months after the intelligence community released its report concluding that the Russian government had attempted to interfere in the 2016 elections and would attempt to do so again.

When the Trump administration's 6 top intelligence officials testified before the Senate that Russia was targeting 2018 elections, this committee, the committee that prides itself on acting in the wake of current issues, followed suit of the House Republican conference by shirking its responsibility to act on this urgent threat.

Ranking Members of the Oversight and Government Reform Committee, the Foreign Affairs Committee, Judiciary Committee, the Permanent Select Committee on Intelligence, the House Armed Services, and the House Administration Committee have all urged the Chairs or Speaker Ryan to aggressively address this on-going National threat. Our calls for action were ignored, responded to with a halfhearted acknowledgment of the threat and a vague promise for future action, or the offer to ask a Government witness about election security at a hearing on another topic.

Because of—our request for thorough hearings and briefings were denied, some committee Democrats joined the Democrats on the Committee of House Administration to form the Congressional Task Force on Election Security. I openly asked Republicans to join us and submit their ideas, yet no Republican Member provided their input or attended the task force's public events.

After studying the topics for 8 months, meeting with stakeholders and holding a series of forums and briefings, the task force produced a report and introduced legislation to implement the recommendations.

Mr. Chairman, I have a stack of requests made by Democrats for action on election security, a copy of the report on legislation I ref-

erenced, and other election security oversight documents, and I ask that they be entered into record at this time.

Chairman MCCAUL. Without objection, so ordered.
[The information follows:]

SUBMITTED FOR THE RECORD BY RANKING MEMBER BENNIE G. THOMPSON

LETTER FROM HONORABLE ENGEL, CONYERS, AND THOMPSON

July 25, 2016.

The Honorable JAMES B. COMEY,
Director of the Federal Bureau of Investigation, FBI Headquarters, 935 Pennsylvania Avenue NW, Washington, DC 20535.

The Honorable ASHTON B. CARTER,
Secretary of Defense, U.S. Department of Defense, 1300 Defense Pentagon, Washington, DC 20301.

The Honorable JOHN F. KERRY,
Secretary of State, U.S. Department of State, 2201 C Street NW, Washington, DC 20520.

The Honorable JAMES R. CLAPPER,
Director of National Intelligence, Office of the Director of National Intelligence, Washington, DC 20511.

DEAR DIRECTOR CORNEY, SECRETARIES KERRY AND CARTER, AND GENERAL CLAPPER: As senior Members of national security committees in Congress, we are deeply troubled by reports of a Russia-supported hacking of Democratic National Committee data, and we applaud the FBI's quick action launching an investigation. We request that the Administration brief Members of Congress on this situation as soon as possible in unclassified or classified settings as needed.

We see two separate issues at play here, both of which deserve the focus of investigators and congressional overseers.

First, the DNC hack was plainly cyber crime. More and more, America's adversaries are employing cyber theft and cyber terrorism as tactics to threaten our security. We need to understand fully the extent of the hack and work to determine who was responsible. We need to assess whose personal information was compromised by the attack and ensure those individuals have what they need to prevent any further damage. We need to determine what vulnerabilities allowed this attack to succeed, and provide information to the public about how to guard against future attacks of this nature.

Second—and perhaps more important—the timing and content of the theft, targeting one of our two major political parties, makes clear that this cyber attack amounts to more than a public embarrassment or harmless mischief. If reports of Russia's involvement are confirmed, the only reasonable conclusion is that leaders in Russia are stealing and disseminating information in an effort to sway an election in the United States.

This is an action right out of President Putin's playbook. In recent years, Russia has influenced elections, infiltrated political parties across Europe, and stoked divisive politics in the hope of fracturing Western unity. It doesn't stretch the imagination that Mr. Putin would now try his hand at manipulating the course of American democracy—leaking information through a syndicate that has repeated anti-Semitic insinuations, endangered lives, and threatened American security by recklessly releasing stolen information. That scenario should sound the alarm for people across this country.

That's why we also ask that the FBI collaborate with the Departments of State and Defense and the Intelligence Community to obtain a complete picture of Russia's involvement and its leaders' intentions. Nearly a half century ago, a break-in at the DNC headquarters eventually led to the end of a Presidency. For a foreign government to engage in the same sort of behavior cannot be tolerated. Russia doesn't get to put its thumb on the scale in our elections. In the days ahead, we need to send a clear message to Russia's leaders and all who mean us harm: we will not allow the Kremlin or any other foreign power to dictate the terms of political debate in this country.

With the clock ticking down to our election, we ask for quick action on this matter. The American people deserve to go to the polls in November confident that Russian subterfuge has had no role in setting the agenda for our country's future.

Sincerely,

ELIOT L. ENGEL,
Ranking Member, House Foreign Affairs Committee.

JOHN CONYERS, JR.,
Ranking Member, House Judiciary Committee.

BENNIE G. THOMPSON,
Ranking Member, House Homeland Security Committee.

LETTER FROM HONORABLE CUMMINGS, CONYERS, ENGEL, AND THOMPSON

August 30, 2016.

The Honorable JAMES COMEY,
Director, Federal Bureau of Investigation, 935 Pennsylvania Avenue NW, Washington, DC 20530.

Dear Mr. Director: Based on multiple press reports, it appears that the Federal Bureau of Investigation (FBI) is investigating whether Russia executed cyber attacks against the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC) that resulted in the illegal hacking of a wide range of emails and other documents.¹

We are writing to request that the FBI assess whether connections between Trump campaign officials and Russian interests may have contributed to these attacks in order to interfere with the U.S. Presidential election.

Serious questions have been raised about overt and covert actions by Trump campaign officials on behalf of Russian interests. It is critical for the American public to know whether those actions may have directly caused or indirectly motivated attacks against Democratic institutions and our fundamental election process.

On July 22, 2016, just days before the Democratic convention, approximately 20,000 pages of illegally hacked documents were leaked by WikiLeaks in an apparent attempt to influence the U.S. Presidential election in favor of Donald Trump.² According to one press report:

"The FBI suspects that Russian government hackers breached the networks of the Democratic National Committee and stole emails that were posted to the anti-secrecy site WikiLeaks on Friday. It's an operation that several U.S. officials now suspect was a deliberate attempt to influence the Presidential election in favor of Donald Trump, according to five individuals familiar with the investigation of the breach."³

Donald Trump has repeatedly praised Russian President Vladimir Putin, stating that "he's doing a great job,"⁴ "I'd get along very well with Vladimir Putin,"⁵ and "It is always a great honor to be so nicely complimented by a man so highly respected."⁶ Donald Trump's business interests in Russia have also been widely reported.⁷

¹ See, e.g., *FBI Investigating Whether Russians Hacked Democratic Party's Emails to Help Donald Trump*, *Los Angeles Times* (July 25, 2016) (on-line at www.latimes.com/nation/la-na-pol-fbi-hack-dnc-russia-20160725-snap-story.html). See also *Growing Evidence Suggests Recent Hacks the Work of Russian-Backed Cyber Militias*, *Fox News* (Aug. 20, 2016) (on-line at www.foxnews.com/politics/2016/08/20/growing-evidence-suggest-recent-hacks-work-russian-backed-cyber-militias.html).

² *WildLeaks Releases Thousands of Documents About Clinton and Internal Deliberations*, *Washington Post* (July 22, 2016) (on-line at www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/).

³ *FBI Suspects Russia Hacked DNC; U.S. Officials Say it Was to Elect Donald Trump*, *Daily Beast* (July 25, 2016) (on-line at www.thedailybeast.com/articles/2016/07/25/fbi-suspects-russia-hacked-dnc-u-s-officials-say-it-was-to-elect-donald-trump.html).

⁴ *Larry King Live*, *CNN* (Oct. 15, 2007) (on-line at www.cnn.com/TRANSCRIPTS/0710/15/lkl.01.html).

⁵ *Donald Trump: "I'd Get Along Very Well With Vladimir Putin,"* *CBS News* (July 30, 2015) (on-line at www.cbsnews.com/news/donald-trump-id-get-along-very-well-with-vladimir-putin/).

⁶ *Trump Says "Great Honor" to Get Compliments from "Highly Respected" Putin*, *ABC News* (Dec. 17, 2015) (on-line at <http://abcnews.go.com/Politics/trump-great-honor-compliments-highly-respected-putin/story?id=35829618>).

⁷ *Inside Donald Trump's Financial Ties to Russia and His Unusual Flattery of Vladimir Putin*, *Washington Post* (June 17, 2016) (on-line at www.washingtonpost.com/politics/inside-trumps-fi).

Donald Trump has proposed shocking policy positions that would greatly benefit Russia, including breaking from longstanding U.S. commitments to our NATO allies to combat Russian aggression⁸ and weakening sanctions and recognizing Russia's annexation of Crimea.⁹

Of direct concern, however, are Donald Trump's comments encouraging Russian hacking and his top aides' previously undisclosed connections to Russian officials and interests.

On July 27, 2016—the third day of the Democratic convention—Donald Trump urged Russia to hack Secretary Hillary Clinton's emails.¹⁰

Less than 2 weeks later, on August 8, 2016, Roger Stone, a Donald Trump confidante, revealed that he has communicated with WikiLeaks founder Julian Assange about the upcoming release of additional illegally hacked Democratic documents. Mr. Stone made these statements during a Republican campaign event while answering a question about a potential "October surprise."¹¹

It is unclear whether U.S. law enforcement authorities have interviewed Mr. Stone about his communications with Mr. Assange or about his knowledge of how WikiLeaks obtained the illegally hacked documents.

In addition, on July 7, 2016, one of Donald Trump's foreign policy advisers, Carter Page, traveled to Moscow to give a speech that was harshly critical of the United States and its "hypocritical focus on ideas such as democratization, inequality, corruption and regime change."¹² Mr. Page had touted his extensive dealings with Russian energy giant Gazprom, claiming that he had been an adviser "on key transactions for Gazprom."¹³ After Donald Trump named Mr. Page as his foreign policy adviser in March, Mr. Page explained that "his business has suffered directly from the U.S. economic sanctions imposed after Russia's escalating involvement in the Ukraine."¹⁴

Mr. Page appears to enjoy high-level access to Russian officials that are currently under sanctions imposed by the United States Government. According to one press report:

"After the Obama administration added Rosneft Chairman Igor Sechin to its sanctions list in 2014, limiting Sechin's ability to travel to the United States or do business with U.S. firms, Page praised the former deputy prime minister, considered one of Putin's closest allies over the past 25 years. Sechin has done more to advance U.S.-Russian relations than any individual in or out of government from either side of the Atlantic over the past decade," Page wrote."¹⁵

It is unclear whether U.S. law enforcement authorities have interviewed Mr. Page about whether he met with Mr. Sechin or other individuals on the U.S. sanctions list during his trip to Moscow or on other occasions.

Another top adviser to Donald Trump, Lt. Gen. Michael Flynn, traveled to Moscow in December 2015 and joined Vladimir Putin at the head table during a dinner honoring the Kremlin-backed media network RT. During the event, General Flynn gave a speech that was highly critical of the United States, stating, "The United

nancial-ties-to-russia-and-his-unusual-flattery-of-vladimir-putin/2016/06/17/dbdcaac8-31a6-11e6-8ff7-7b6c1998b7a0_story.html?postshare=1821472042965377&tid=ss_mail).

⁸ *Trump Takes Heat from NATO Officials for Interview Comments*, Fox News (July 21, 2016) (on-line at www.foxnews.com/politics/2016/07/21/trump-takes-heat-from-nato-officials-for-interview-comments.html).

⁹ *This Week with George Stephanopoulos*, ABC News (July 31, 2016) (on-line at <http://abcnews.go.com/Politics/week-transcript-donald-trump-vice-president-joe-biden/story?id=41020870>).

¹⁰ *Trump Urges Russia to Hack Clinton's Email*, Politico (July 27, 2016) (on-line at www.politico.com/story/2016/07/trump-putin-no-relationship-226282).

¹¹ *Trump Ally Claims He "Communicated With" WikiLeaks Founder*, Washington Examiner (Aug. 9, 2016) (on-line at www.washingtonexaminer.com/trump-ally-claims-he-communicated-with-wikileaks-founder/article/2598931).

¹² *Trump's Russia Adviser Criticizes U.S. for "Hypocritical Focus on Democratization," Washington Post* (July 7, 2016) (on-line at www.washingtonpost.com/world/europe/trumps-russia-adviser-criticizes-us-for-hypocritical-focus-on-democratization/2016/07/07/804a3d60-4380-11e6-a76d-3550dba926ac_story.html).

¹³ *Biography of Carter Page, CFA, Global Energy Capital LLC* (accessed Aug. 22, 2016) (on-line at www.globalenergycap.com/management/).

¹⁴ *Trump's New Russia Adviser Has Deep Ties to Kremlin's Gazprom*, Bloomberg (Mar. 30, 2016) (on-line at www.bloomberg.com/politics/articles/2016-03-30/trump-russia-adviser-carter-page-interview).

¹⁵ *Trump Adviser's Public Comments, Ties to Moscow Stir Unease in Both Parties*, Washington Post (Aug. 5, 2016) (on-line at www.washingtonpost.com/business/economy/trump-advisers-public-comments-ties-to-moscow-stir-unease-in-both-parties/2016/08/05/2e8722fa-5815-11e6-9aee-8075993d73a2_story.html).

States can't sit there and say, 'Russia, you're bad.'" ¹⁶ The following week, President Putin praised Donald Trump as "an outstanding and talented personality."¹⁷ General Flynn declined to answer media inquiries about whether he traveled to Moscow on Donald Trump's behalf.¹⁸

Most recently, Donald Trump's campaign chairman, Paul Manafort, resigned after failing to disclose his role in assisting a pro-Russian party in Ukraine. Mr. Manafort reportedly had "wooded investments from oligarchs linked to Putin and advised the now-toppled pro-Russian Ukrainian president Viktor Yanukovich."¹⁹ According to one press account:

"Donald Trump's campaign chairman helped a pro-Russian governing party in Ukraine secretly route at least \$2.2 million in payments to two prominent Washington lobbying firms in 2012, and did so in a way that effectively obscured the foreign political party's efforts to influence U.S. policy. . . . Under Federal law, U.S. lobbyists must declare publicly if they represent foreign leaders or their political parties and provide detailed reports about their actions to the Justice Department. A violation is a felony and can result in up to 5 years in prison and a fine of up to \$250,000."²⁰

Rick Gates, a top strategist in Donald Trump's campaign, reportedly worked with Mr. Manafort on this effort, "helping steer the advocacy work done by a pro-Yanukovich nonprofit," including "downplaying the necessity of a Congressional resolution meant to pressure the Ukrainian leader to release an imprisoned political rival."²¹ Although Mr. Manafort has resigned from his position, it appears that Mr. Gates continues to be a top adviser to Mr. Trump.

It is unclear whether U.S. law enforcement authorities have interviewed Mr. Manafort or Mr. Page about their failure to disclose this information, but several prominent members of Mr. Trump's party have expressed grave concerns.

For example, Republican Adam Kinzinger of Illinois called for an investigation into Donald Trump's "chief adviser, what his association with the Russians are." More broadly, Rep. Kinzinger criticized "this affection in the campaign for Russia and Vladimir Putin," and he questioned how and why a reference to Russian offensive weapons was mysteriously removed from the Republican Party's platform, noting that "it just happened."²²

Similarly, Eliot Cohen, who served as a counselor at the State Department under the George W. Bush administration, warned: "Foreign governments sometimes express preferences about who should be elected; that's already problematic. But to do something in the nature of dirty tricks would be a very, very serious problem."²³

Finally, House Speaker Paul Ryan's spokesman stated: "Russia is a global menace led by a devious thug. Putin should stay out of this election."²⁴

¹⁶ *Trump Embraces Ex-Top Obama Intel Official*, *Daily Beast* (Mar. 9, 2016) (on-line at www.thedailybeast.com/articles/2016/03/09/donald-trump-embraces-top-obama-intel-official.html).

¹⁷ *Putin Praises "Bright and Talented" Trump*, CNN (Dec. 17, 2015) (on-line at www.cnn.com/2015/12/17/politics/russia-putin-trump/).

¹⁸ *Trump Embraces Ex-Top Obama Intel Official*, *Daily Beast* (Mar. 9, 2016) (on-line at www.thedailybeast.com/articles/2016/03/09/donald-trump-embraces-top-obama-intel-official.html).

¹⁹ *Trump Adviser's Public Comments, Ties to Moscow Stir Unease in Both Parties*, *Washington Post* (Aug. 5, 2016) (on-line at www.washingtonpost.com/business/economy/trump-advisers-public-comments-ties-to-moscow-stir-unease-in-both-parties/2016/08/05/2e8722fa-5815-11e6-9aee-8075993d73a2_story.html).

²⁰ *Manafort Tied to Undisclosed Foreign Lobbying*, Associated Press (Aug. 17, 2016) (on-line at <http://bigstory.ap.org/article/c01989a47ee5421593ba1b301ec07813/ap-sources-manafort-tied-undisclosed-foreign-lobbying>).

²¹ *Id.*

²² *GOP Congressman Warns Trump: Russia Not an Ally*, CNN (Aug. 6, 2016) (on-line at www.cnn.com/videos/tv/2016/08/15/gop-congressman-rep-adam-kinzinger-reacts-to-trumps-isis-plan-the-lead.cnn); Rep. Kinzinger Calls for Investigation Into Manafort-Russian Ties, *Politico* (Aug. 6, 2016) (on-line at www.politico.com/story/2016/08/gop-rep-calls-for-investigation-into-manafort-russian-ties-227090). See also *Donald Trump Campaign Chairman Paul Manafort Resigns*, CNN (Aug. 20, 2016) (on-line at www.cnn.com/2016/08/19/politics/donald-trump-campaign-chairman-paul-manafort-resigns/index.html) (citing Rep. Sean Duffy of Wisconsin, stating, "I want to know what money he got from a pro-Russian organization in the Ukraine.").

²³ *Trump Invites Russia to Meddle in the US Presidential Race with Clinton's Emails*, *Washington Post* (July 27, 2016) (on-line at www.washingtonpost.com/politics/trump-invites-russia-to-meddle-in-the-us-presidential-race-with-clintons-emails/2016/07/27/a85d799e-5414-11e6-b7de-dfe509430c39_story.html?tid=a_inl).

²⁴ *Speaker Paul Ryan Calls on "Global Menace" Russia to "Stay Out of This Election;" The Call Came After Donald Trump Encouraged Russian Hackers to Target Hillary Clinton*, CNN

We do not know if Donald Trump's public statements or the connections of his campaign officials to Russian interests directly or indirectly led to the cyber attacks against Democratic party organizations, but there is wide-spread agreement that the United States should take all steps possible to prevent Russia from interfering in our electoral process and prosecute to the full extent of the law anyone involved in such a scheme.

Thank you for your consideration of this request.

Sincerely,

ELIJAH E. CUMMINGS,
Ranking Member, Committee on Oversight and Government Reform.

JOHN CONYERS, JR.,
Ranking Member, Committee on the Judiciary.

ELLIOT L. ENGEL,
Ranking Member, Committee on Foreign Affairs.

BENNIE G. THOMPSON,
Ranking Member, Committee on Homeland Security.

LETTER FROM HONORABLE JACKSON LEE

August 31, 2016.

The Honorable MICHAEL MCCAUL,
Chairman, Committee on Homeland Security Washington, DC 20515.

The Honorable BENNIE THOMPSON,
Ranking Member, Committee on Homeland Security Washington, DC 20515.

DEAR CHAIRMAN MCCAUL AND RANKING MEMBER THOMPSON: As a Senior Member of the House Committee on Homeland Security, I am writing to request that the committee convene a joint briefing with the Select Committee on Intelligence, Foreign Affairs, and House Administration to discuss specific threats to the U.S. election systems from outside influences. It has been reported that attempts have already been made to compromise the integrity of State-wide voter registration databases for Illinois and Arizona.

On August 15, Homeland Security Secretary Jeh Johnson held a conference call with the National Association of Secretaries of State and election officials to discuss the election infrastructure cybersecurity. During that call Secretary Johnson offered Federal assistance to State officials in managing risks to voting systems in their jurisdiction.

State-wide centralized voter registration systems are used by many States during elections to authenticated voters to determine who can cast a ballot. One of the threats to the election system would be a "denial of service" attack that prevents local polling locations from accessing information on registered voters.

For these reasons, I believe that it is important that a joint briefing with the Select Committee on Intelligence, Foreign Affairs, and House Administration be held at the earliest possible time.

If you have questions regarding this request, please contact me through my Homeland Security Policy Advisor, Lillie Coney.

Very Truly Yours,

SHEILA JACKSON LEE,
MEMBER OF CONGRESS.

LETTER FROM SEVEN MEMBERS OF CONGRESS

December 6, 2016.

President BARACK OBAMA,
The White House, 1600 Pennsylvania Avenue NW, Washington, DC 20500.

DEAR MR. PRESIDENT: We are deeply concerned by Russian efforts to undermine, interfere with, and even influence the outcome of our recent election. This Russian malfeasance is not confined to us, but extends to our allies, our alliances and to democratic institutions around the world.

The integrity of democracy must never be in question, and we are gravely concerned that Russia may have succeeded in weakening Americans' trust in our electoral institutions through their cyber activity, which may also include sponsoring

(July 27, 2016) (on-line at <http://time.com/4426783/paul-ryan-republicans-donald-trump-russia/>).

disclosures through WikiLeaks and other venues, and the production and distribution of fake news stories.

Foreign interference presents a win-win for Russia—which we must counter. By eroding Americans’ and foreigners’ trust in U.S. institutions, Russia both weakens our country and sows global instability and uncertainty. Both present a boon for Russia and a loss for those working to maintain peace and prosperity around the world through the leadership of the United States and its allies.

To evaluate Congress’s response appropriately, we would like all Members to have a comprehensive understanding of what the U.S. intelligence community knows regarding Russia’s involvement in these actions and attempts to interfere in our election. Specifically, we are requesting a classified briefing that will provide details regarding Russian entities’ hacking of American political organizations; hacking and strategic release of emails from campaign officials; the WikiLeaks disclosures; fake news stories produced and distributed with the intent to mislead American voters; and any other Russian or Russian-related interference or involvement in our recent election.

We thank you for your attention to this matter.

Sincerely,

STENY H. HOYER,
Democratic Whip.

JOHN CONYERS,
Ranking Member, Committee on Judiciary.

ELIOT ENGEL,
Ranking Member, Committee on Foreign Affairs.

BENNIE G. THOMPSON,
Ranking Member, Committee on Homeland Security.

ELIJAH CUMMINGS,
Ranking Member, Committee on Oversight and Government Reform.

ADAM SMITH,
Ranking Member, Committee on Armed Services.

ADAM SCHIFF,
Ranking Member, Permanent Select Committee on Intelligence.

LETTER FROM HONORABLE JACKSON LEE

December 13, 2016.

The Honorable MICHAEL McCAUL,
Chairman, Committee on Homeland Security, 176 Ford HOB, Washington, DC 20515.

The Honorable BENNIE THOMPSON,
Ranking Member, Committee on Homeland Security, H2-117 Ford HOB, Washington, DC 20515.

DEAR CHAIRMAN McCAUL AND RANKING MEMBER THOMPSON: As a Member of the standing Committee on Homeland Security since its creation, I am writing to respectfully request that the committee conduct thorough and probing hearings regarding the activities of entities allied with the Government of Russia to influence the outcome of the 2016 presidential election in the United States when the 115th Congress convenes in January 2017.

Given your strong commitment to the rule of law and constitutional governance, and your demonstrated record of working together constructively, I know you find it as deeply disturbing as I do that the Central Intelligence Agency has concluded, in a secret assessment, that Russia intervened in the 2016 election to help Donald Trump win the presidency, rather than just to undermine confidence in the U.S. electoral system.

This is as grave an attack on American independence and sovereignty as Pearl Harbor and 9/11. It cannot be allowed to stand with impunity. The facts and actors involved in this plot must be uncovered and laid bare for the American people to see and understand.

The Office of the Director of National Intelligence, which includes the Central Intelligence Agency, has cited a growing body of intelligence from multiple sources confirming that the politically motivated hacks of the 2016 election originated at the highest levels of the Kremlin and confirmed that the activity was intended to favor Presidential candidate Trump. This election malfeasance on the part of the Government of Russia appears to be part of wider strategy to disrupt and destabilize the political system and economies of the western democracies.

The integrity of the democratic process must never be in question, and I am very concerned that Russian interference in the recent election may have inflicted substantial damage to Americans' confidence in the political system. That interference includes, but is not limited to sponsoring disclosures through WikiLeaks and other venues, the production and distribution of fake news stories to influence traditional and social media, and cyber attacks on computing networks used by local and State election administrations and political organizations to communicate with voters, constituents, and other members of the public.

Foreign interference in U.S. elections also represents a serious threat to National security to the full enjoyment and exercise of the civil liberties and rights Americans justly value and cherish. There can be no higher priority for the next Congress than ensuring that the election process, the hallmark of this democratic republic's governance, is invulnerable to foreign influence or manipulation.

Specifically, the House Homeland Security Committee should investigate the findings of the intelligence community through a comprehensive, or "deep-dive," investigation of the cyber attacks that plagued the 2016 Presidential election, including cyber attacks previously designed to undermine the campaign of the Democratic Presidential candidate which were previously determined by the U.S. intelligence community to be connected to entities allied with the Government of Russia. Further, the hearings should explore the impact, if any, that media reporting of WikiLeaks data breach information had on voter decisions in the 2016 election and the influence of "fake news," false stories deliberately injected into the news mainstream to mislead and misinform voters, such as the Comet Ping Pong incident which led a North Carolina man to fire rounds from an AR-15 rifle into a crowd at a pizzeria in Washington, DC.

The linchpin of representative democracies such as the United States is public confidence in the political system, regime, and community. That confidence in turn rests upon the extent to which the public has faith that the system employed to select its leaders accurately reflects its preferences. At bottom, this means that the American people must be able to freely elect their leaders without interference, covert or overt, from foreign governments or entities allied with foreign powers.

For these reasons, it is essential that when the 115th Congress convenes in January 2017, the Committee on the Homeland Security conduct thorough and probing inquiry regarding the activities of entities allied with the Government of Russia to influence the outcome of the 2016 U.S. Presidential election.

Thank you for your consideration of this urgent request. If you have questions or need further information, contact me through my Chief of Staff, Glenn Rushing.

Very Truly Yours,

SHEILA JACKSON LEE,
MEMBER OF CONGRESS.

LETTER FROM HONORABLE THOMPSON AND RICHMOND

May 23, 2017.

President DONALD J. TRUMP,
The White House, 1600 Pennsylvania Avenue, NW Washington, DC 20500.

DEAR MR. PRESIDENT: Last week, reports surfaced that the White House may be planning to create a false narrative about the Department of Homeland Security's Automated Indicator Sharing (AIS) program in order to neutralize criticism over your handling of classified information with Russian officials.¹

According to a piece in *Foreign Policy* (FP), White House officials met last Wednesday to discuss the possibility of planting a story in the media or opening an investigation to accuse DHS of using the AIS platform to "inappropriately open up streams of sensitive data to Russia and other nonallies."² These officials hoped to create the illusion that AIS, a public-facing portal that does not deal in classified information, exhibits careless information practices by the Obama administration roughly equivalent to your disclosure of intelligence gathered by a foreign ally. A second source confirmed that "Trump and his team have been interested in targeting the Homeland Security program for the past couple weeks. Nothing has been decided . . . but it's an option on the table."³

¹ Foreign Policy, "Trump Team Planning Possible Retaliation for Classified Leak Allegation," by Jenna McLaughlin (May 18, 2017), <http://foreignpolicy.com/2017/05/18/trump-team-planning-possible-retaliation-for-classified-leak-allegations/>.

² Id. (quoting the article, not the source).

³ Id. (quoting the article, not the source).

These reports, if true, are deeply troubling. The AIS program is the result of bipartisan legislation enacted in the 114th Congress, after years of negotiation between privacy, security, and industry stakeholders in an effort to speed public-private sharing of cyber threat indicators. In a press release celebrating AIS' launch last year, DHS described the capability as "the 'See Something, Say Something' of the internet," noting that:

"When one participant detects a threat, all participants in AIS will learn about it. By broadening the depth and increasing the speed of cybersecurity information sharing, the country as a whole will be better able to manage cyber threats. The Cybersecurity Act of 2015 also provides targeted liability protection to companies that share cyber threat indicators with DHS or with each other. And like all of the Department's cybersecurity programs, AIS includes rigorous privacy and civil liberties protections."⁴

Despite holding enormous promise, AIS is still in its nascent stages. The Department should be using its limited resources to grow the capability and build trusted partnerships with its customer base, rather than fighting off baseless accusations. While we sincerely hope that the accounts in the FP report are not true, we nevertheless cannot stand aside and allow the White House to jeopardize this important program in a self-serving attempt to change the news cycle.

Pursuant to Rule X(3)(g) and Rule XI of the Rules of the House of Representatives, we respectfully request you provide a written response to the following information, and whatever supplementary information you deem responsive, by June 1, 2017.

1. Please provide a detailed log of meetings held at the White House on Wednesday, May 17, 2017, accompanied by a list of attendees. If the meeting described herein, with respect to DHS' Automated Indicator Sharing program, indeed occurred, please provide any notes, discussion drafts, or other materials generated in advance of, during, or subsequent to the discussion.

2. Please provide the dates, times, and attendees of any meetings White House officials have held where DHS cybersecurity information sharing programs, including the Automated Indicator Sharing program, may have been discussed.

3. Has the White House directed an investigation into how the DHS Automated Indicator Sharing program shares cyber threat information with its partners, including international partners? If so, on what grounds?

4. If the White House is considering or considered planting a false story about the Automated Indicator Sharing program, as indicated in the FP piece, please provide any meeting notes, drafts, and other related materials that describe the details of such a story.

Thank you for your attention to this matter. If you have any questions, please contact Hope Goins, Minority Staff Director.

BENNIE G. THOMPSON,
Ranking Member.

CEDRIC L. RICHMOND,
Ranking Member, Subcommittee on Cybersecurity & Infrastructure Protection.

LETTER FROM RANKING MEMBER BENNIE G. THOMPSON

May 23, 2017.

The Honorable MICHAEL T. MCCAUL,
*Chairman, Committee on Homeland Security, H2-176 Ford House Office Building,
Washington, DC 20515.*

DEAR CHAIRMAN MCCAUL: I am writing to express my continued commitment to examining the Russian government's interference in the 2016 elections.

On April 5, during the consideration of a measure to jumpstart an investigation into what the Department of Homeland Security knew and did about this unprecedented attack on our democracy (H. Res. 235), you indicated that, while you opposed my resolution of inquiry, you supported examining this issue through the normal committee process. At the time, you suggested that Members could ask DHS Secretary Kelly about Russian interference when he testifies next before the committee. While asking one-off questions of the Secretary at a public hearing of Government officials in a closed-door meeting here or overseas may yield some information, it

⁴DHS "Open for Business to Receive Cyber Threat Indicators at Machine Speed," (March 17, 2016), <https://www.dhs.gov/blog/2016/03/17/dhs-open-business-receive-cyber-threat-indicators-machine-speed>.

does not replace the need for a comprehensive investigation. The gravity of this matter demands more; it demands that the committee launch a bipartisan investigation—particularly given recent developments surrounding the Russia investigation.

Following President Trump’s abrupt firing of FBI Director Comey earlier this month, a special counsel was appointed by the Deputy Attorney General to oversee the investigation, which FBI Director Comey initiated, into Russian meddling in our elections. Since then, the drumbeat for an independent commission that cannot be interfered with by the Trump administration steadily intensified. As I said during my opening statement when H. Res. 235 was considered, current investigations under way in Congress and at the Justice Department are not likely to focus on DHS’s efforts—which are important to evaluate given that the Russians are expected to attempt to interfere in future U.S. elections. As such, now is the time for this committee to launch its own bipartisan inquiry.

I share the view that you expressed at our April markup that any foreign government interference in our elections is unacceptable and should not go unpunished. By launching a committee investigation, we could do our part to ensure not only that those involved are punished but that State officials responsible for overseeing our elections have the answers they need to guard against future interference. Protecting our election systems has been and will continue to be a bipartisan issue. I truly hope that we can begin to address this matter with the seriousness that it deserves, and look forward to working with you to undertake oversight into DHS’s efforts to identify and mitigate harm to our election systems.

Thank you for your time and attention to this matter. If you have any questions, please contact Rosaline Cohen, Chief Counsel for Legislation.

Sincerely,

BENNIE G. THOMPSON,
Ranking Member.

LETTER FROM TWELVE MEMBERS OF CONGRESS

June 21, 2017.

The Honorable JOHN F. KELLY,
Secretary, U.S. Department of Homeland Security, Washington, DC 20528.

DEAR SECRETARY KELLY: We write to express our concern regarding recent statements you have made with respect to the designation of election infrastructure as a critical infrastructure subsector and to seek clarification regarding what you envision the Department of Homeland Security’s (the Department or DHS) role to be when it comes to securing election infrastructure.

On January 6, 2017, the Office of the Director of National Intelligence (ODNI) released a report, completed in coordination with the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA), entitled *Background to “Assessing Russian Activities and Intentions in Recent US Elections”*: *The Analytic Process and Cyber Incident Attribution*. The declassified version of the report made several concerning findings related to the depth and breadth of Russia’s efforts to interfere in the 2016 Presidential elections, including that “Russian intelligence obtained and maintained access to elements of multiple US State or local electoral boards.”¹ Ultimately, the ODNI assessed that “Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US Presidential election to future influence efforts worldwide, including against US allies and their election processes.”²

The same day, your predecessor, then-Secretary Jeh Johnson, designated election infrastructure as critical infrastructure.³ In making the designation, then-Secretary Johnson stated:

¹ Office of the Director of National Intelligence, *Background to “Assessing Russian Activities and Intentions in Recent US Elections”*: *The Analytic Process and Cyber Incident Attribution*, (Jan. 6, 2017), available at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

² *Id.*

³ Statement by U.S. Department of Homeland Security Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, (Jan. 6, 2017), available at <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>. “Election Infrastructure” includes: “storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of State and local governments.” *Id.*

"I have determined that election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector. Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law.

"I have reached this determination so that election infrastructure will, on a more formal and enduring basis, be a priority for cybersecurity assistance and protections that the Department of Homeland Security provides to a range of private and public sector entities."⁴

Importantly, then-Secretary Johnson made clear that a State or local election board's decision to avail itself of DHS' cybersecurity resources is voluntary. The designation allows the Department "to prioritize our cybersecurity assistance to [S]tate and local election officials, but only for those who request it."⁵

"In light of the mounting evidence that Russia sought to interfere with the 2016 election to both sway the outcome and erode public confidence in our democratic institutions—an objective it had pursued for over a decade—we supported the designation of election infrastructure as a critical infrastructure subsector and were interested in ensuring that the new administration would continue to prioritize cybersecurity assistance to State and local election officials. Accordingly, when you first testified before our Committee on February 7, 2017, you were asked about your views on the critical infrastructure subsector designation. You assuaged our concern that the administration might rescind the designation when you responded: 'I believe we should help all of the [S]tates—provide them as much help as we can to make sure that their systems are protected in future elections. So, I would argue that, yes, we should keep that in place.'⁶

Four months later, you testified before our committee once again. This time, your remarks called into question your commitment to honor the designation of election infrastructure as critical infrastructure. You stated:

"My predecessor, Jeh Johnson, just before he left, designated the whole system as critical infrastructure. I've had a lot of push-back from [M]embers of Congress, both sides of the aisle. Governors have pushed back on that . . . I'm meeting with all of the Homeland Security—I believe it's next week—their Homeland Security [S]tate advisors. This will be a topic that we'll bring up about do they feel it's needed. But by no means do we have any intention, desire, or move to take over any [S]tate process or tell the [S]tates how to do business."⁷

Aside from the resistance you have described from some Members of Congress and State officials, it is hard to understand what has changed since you testified in February that would establish reasonable grounds to reconsider the designation. Indeed, the only new information to emerge in the interim is even more disturbing evidence regarding the scope and breadth of Russian efforts to disrupt the 2016 elections. And, to disabuse Congress of the notion that Russia's interference in the 2016 elections was an isolated incident, then-FBI Director James Comey warned the House Permanent Select Committee on Intelligence in March: "[T]hey'll be back. And they'll be back in 2020. They may be back in 2018."⁸

Since the beginning of the month, news reports have revealed that Russia's efforts to penetrate election systems was far more successful in scope than previously understood, and involved sending spearfishing emails to over 100 election officials to gain access to their networks.⁹ Investigators in Illinois found evidence Russian hackers gained access to software designed to be used by poll workers on Election Day in the summer and fall of 2016 and attempted to delete or alter voter data.

⁴Id.

⁵Id.

⁶*Ending the Crisis: America's Borders and the Path to Security Before H Comm. On Homeland Security*, 115th Cong. (Feb. 7, 2017) (statement of John F. Kelly, Secretary, Department of Homeland Security), available at <http://www.cq.com/doc/congressionaltranscripts-5036886?14>.

⁷Department of Homeland Security Reauthorization and the President's Fiscal Year 2018 Budget Request, Before H. Comm. On Homeland Security, 115th Cong. (June 7, 2017) (statement of John F. Kelly, Secretary, Department of Homeland Security), available at <http://www.cq.com/doc/congressionaltranscripts-5119108?4>.

⁸"Full Transcript: FBI Director James Comey Testifies on Russian Interference in 2016 Election," *The Washington Post* (Mar. 20, 2017), available at https://www.washingtonpost.com/news/post-politics/wp/2017/03/20/full-transcript-fbi-director-james-comey-testifies-on-russian-interference-in-2016-election/?utm_term=.a3209228adef.

⁹Matthew Cole et. al, "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," *The Intercept* (June 5, 2017), <https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/> (last accessed June 21, 2017).

Hackers compromised 90,000 records in Illinois, and gained access to the State voter database that included names, dates of birth, genders, driver's licenses, and partial Social Security numbers on 15 million people.¹⁰

We agree with you that “there is nothing more fundamental to our democracy than voting,”¹¹ and we must protect against efforts to undermine public confidence in our cherished democratic institutions. There is no evidence that attempts to interfere in our elections—be it Russia, another State actor, or a non-State actor—are declining, and the cybersecurity threats to election infrastructure are only growing more complex. It is more important than ever that State and local election officials are able to rely on assistance from the Department of Homeland Security when they need it.

Toward that end, we urge you to not to back down from your commitment to honor the designation of election infrastructure as a critical infrastructure subsector, and we stand ready to assist you in your efforts to educate concerned States on the meaning of this designation. We look forward to working with you to help DHS do its part to ensure the integrity of our election systems.

Sincerely,

BENNIE G. THOMPSON,
Ranking Member, House Committee on Homeland Security.
SHEILA JACKSON LEE,
Member, House Committee on Homeland Security.
JAMES R. LANGEVIN,
Member, House Committee on Homeland Security.
CEDRIC L. RICHMOND,
Member, House Committee on Homeland Security.
WILLIAM R. KEATING,
Member, House Committee on Homeland Security.
DONALD M. PAYNE, JR.,
Member, House Committee on Homeland Security.
FILEMON VELA,
Member, House Committee on Homeland Security.
BONNIE WATSON COLEMAN,
Member, House Committee on Homeland Security.
KATHLEEN M. RICE,
Member, House Committee on Homeland Security.
J. LUIS CORREA,
Member, House Committee on Homeland Security.
VAL B. DEMINGS,
Member, House Committee on Homeland Security.
NANETTE D. BARRAGÁN,
Member, House Committee on Homeland Security.

LETTER FROM HONORABLE BRADY AND THOMPSON

November 16, 2017.

The Honorable RODNEY P. FRELINGHUYSEN,
Chairman, Committee on Appropriations.

The Honorable NITA M. LOWEY,
Ranking Member, Committee on Appropriations.

DEAR CHAIRMAN FRELINGHUYSEN AND RANKING MEMBER LOWEY: As you and your colleagues prepare to finalize appropriations legislation for fiscal year 2018, we respectfully request that you appropriate the remaining \$400 million from the Help America Vote Act of 2002 (HAVA) for States to use to secure their elections infra-

¹⁰Michael Riley and Jordan Robertson, “Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known,” *Bloomberg* (June 13, 2017), <https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections> (last accessed June 21, 2017).

¹¹*The Department of Homeland Security Fiscal Year 2018 Budget Request Before S. Comm. on Homeland Security* 115th Cong. (June 6, 2015), (statement of John F. Kelly, Secretary, Department of Homeland Security), available at <http://www.cq.com/doc/congressionaltranscripts-5116103?7>.

structure.¹ We know now that Russia launched an unprecedented assault on our elections in 2016, targeting 21 States' voting systems, and we believe this money is necessary to protect our elections from future attack.

Over the past 5 months, we have co-chaired an Election Security Task Force to better understand what can be done to protect our elections going forward. Our findings demonstrate that there is an urgent need for Federal funding to help States secure their elections.

Through our investigation, we found that voting machines can easily be hacked. In July, at DefCon, one of the world's largest, longest-running, and best-known hacker conferences, 25 pieces of election equipment were successfully breached by participants with little prior knowledge and limited tools.² In over 40 States, elections are carried out using voting machines that were purchased more than a decade ago.³ These machines are now either obsolete or at the end of their useful life. Some of these machines rely on operating systems like Windows XP or Windows 2000 which pose a particularly significant security risk as those operating systems either do not receive regular security patches, or have stopped receiving support altogether.⁴ These issues are exacerbated by the fact that 20 percent of Americans cast their ballot on voting machines that do not have any kind of paper backup.⁵ In other words, if these paperless machines were hacked, it would be nearly impossible to tell.⁶

State voter registration databases are also vulnerable to attack. In Illinois, hackers successfully breached registration databases and attempted, but failed, to alter and delete voting records.⁷ In Arizona, hackers successfully installed malware on a county election official's computer.⁸ Russian hackers also targeted at least one election vendor with the hope of ultimately obtaining access into numerous State and local voter registration databases.⁹ If these attacks had been successful, hackers would have been able to alter or delete voter registration records, causing a great deal of chaos on Election Day and potentially swaying the results of the election.

The single most urgent need is for States using paperless machines to replace their outdated equipment with paper ballot voting systems. The Brennan Center estimates that cost to replace paperless voting machines would be between \$130 and \$400 million, and States do not have the money to do this themselves.¹⁰ South Carolina is 1 of the 5 remaining States that relies exclusively on paperless machines, and a spokesman for the South Carolina Election Commission recently told the *New York Times*, "We're using the same equipment we've used since 2004. If \$40 million dropped into our hands today, we'd have a paper ballot trail, too."¹¹ In order to prevent future attacks, States also need to hire IT staff to upgrade and maintain IT infrastructure, and train election officials and poll workers on cybersecurity.

State and local election officials are acutely aware that they need to improve election security, but they lack the necessary funds to safeguard their voting infrastructure.¹² In most States, legislatures are not increasing their election security budgets.¹³ In some cases, Governors are actively undermining election security efforts. In Florida, Governor Scott's budget proposed reducing the funding for the Division of

¹ Pub. L. 107-252 (Oct. 29, 2002).

² Matt Blaze et al., *DEFCON 25 Voting Machine Hacking Village: Rep. on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, 4 (2017) <https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf>.

³ Lawrence Norden & Ian Vanderwalker, Brennan Center for Justice at NYU School of Law, *Securing Elections from Foreign Interference*, 9 (2017).

⁴ Id.

⁵ Norden & Vandewalker, 11.

⁶ Eric Geller, *Virginia Bars Voting Machines Considered Top Hacking Target*, *POLITICO* (Sept. 8, 2017) <http://www.politico.com/story/2017/09/08/virginia-election-machines-hacking-target-242492>.

⁷ Pam Fessler, *10 Months After Election Day, Feds Tell States More About Russian Hacking*, *NPR* (Sept. 22, 2017) <https://www.npr.org/2017/09/22/552956517/ten-months-after-election-day-feds-tell-states-more-about-russian-hacking>.

⁸ Id.

⁹ Matthew Cole, et. al., *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, *The Intercept*, (June 5, 2017) <https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/>.

¹⁰ Norden & Vandewalker, 11.

¹¹ Michael Wines, *Wary of Hackers, States Move to Upgrade Voting Systems*, *The New York Times* (October 14, 2017) <https://www.nytimes.com/2017/10/14/us/voting-russians-hacking-states.html?r=0>.

¹² Reid Wilson, *Election Officials Race To Combat Cyberattacks*, *The Hill* (Nov. 8, 2017) <https://thehill.com/homenews/campaign/359243-election-officials-race-to-combat-cyberattacks>.

¹³ Cory Bennett et. al., *Cash-strapped States Brace for Russian Hacking Fight*, *POLITICO* (Sept. 3, 2017) <https://www.politico.com/story/2017/09/03/election-hackers-russia-cyberattack-voting-242266>.

Elections by almost \$1 million.¹⁴ In July, Governor Kasich vetoed a provision in Ohio's budget that would have allocated \$1 million toward voting equipment.¹⁵ Governor Walker issued a partial veto to the State's budget, and in doing so, eliminated five jobs from the Wisconsin Elections Commission.¹⁶ This issue is simply too important to sit back and watch State governments and the Federal Government pass responsibility back and forth.

Moreover, State and local officials have expressed a desire for Congress to step in. In a recent *Politico* survey of State election officials, 21 of 33 respondents want the Federal Government to authorize funds for States to spend on replacing voting machines or otherwise strengthening election security.¹⁷ In response to the letter sent out by the Task Force to the chief election official in each State asking how the Federal Government could help States with election security, the National Association of Secretaries of States replied by saying, "States would clearly benefit from the appropriation of the outstanding balance of Federal HAVA funds to aid them in ensuring that they have sufficient equipment, technical support, and resources to maintain a sound security posture for their computer-based systems."¹⁸

The money that States need can be appropriated right now. HAVA authorized \$3 billion dollars for States to upgrade and modernize their election infrastructure in the wake of the chaotic 2000 Presidential election. According to the Election Assistance Commission, the agency charged with administering HAVA's grants, approximately \$2.6 billion of the HAVA funds have been distributed.¹⁹ Appropriating the remaining \$400 million would enable States to take the crucial security steps of replacing outdated equipment, implementing cybersecurity best practices, and hiring IT staff.

When a sovereign nation attempts to meddle in our elections, it is an attack on our country. We cannot leave States to defend against the sophisticated cyber tactics of state actors like Russia on their own. Michael Chertoff, former Secretary of Homeland Security wrote in *The Wall Street Journal*, "In an age of unprecedented cyber risks, these dangers aren't surprising. But lawmakers and election officials' lackadaisical response is both staggering and distressing . . . This is a matter of National security, and Congress should treat it as such." We urge you to recognize that ensuring the security and integrity of our election system is a bipartisan issue, and to appropriate the funds States desperately need to secure their elections.

Thank you for your attention to this matter.

Sincerely,

ROBERT A. BRADY,
Ranking Member, Committee on House Administration, U.S. House of Representatives.

BENNIE G. THOMPSON,
Ranking Member, Committee on Homeland Security, U.S. House of Representatives.

LETTER FROM SIX MEMBERS OF CONGRESS

January 9, 2018.

The Honorable PAUL D. RYAN,
Speaker of the House of Representatives, United States Capitol, Washington, DC 20515.

DEAR MR. SPEAKER: January 6 marked 1 year since the Office of the Director of National Intelligence released its ominous report documenting Russia's multifaceted campaign to interfere in the 2016 elections and warning that Russia is likely to do it again.

¹⁴ Governor Rick Scott's 2017–2018 Budget, (last visited, Oct. 18, 2017) <http://fightingforfloridasfuturebudget.com/web%20forms/Budget/BudgetService.aspx?rid=327714&rid2=298915&ai=45000000&title=STATE>.

¹⁵ Jackie Borchardt, *Ohio Gov. John Kasich Vetoes Medicaid Freeze, Signs State Budget Bill*, Cleveland.com (July 10, 2017) https://www.cleveland.com/metro/index.ssf/2017/06/ohio_gov_john_kasich_signs_sta.html.

¹⁶ Veto Message in Brief, Sept. 20, 2017, p. 13. <https://walker.wi.gov/sites/default/files/09.20.17%20Veto%20Message%20in%20Brief.pdf>.

¹⁷ Bennett.

¹⁸ Letter From Connie Lawson, President, National Association of Secretaries of State, to Congressman Bennie Thompson & Congressman Robert Brady, Co-Chairman, Joint Task Force on Election Security (Aug. 3, 2017) (on file with author).

¹⁹ U.S. Election Assistance Commission, *Annual Grant Expenditure Report Fiscal Year 2015*, 6 <https://www.eac.gov/documents/2016/4/11/final-fy-2015-grants-reportpdf/>.

Over the past year, our Nation has learned more about the breadth and magnitude of Russia's growing threat against our democracy and our National security. We now know that Russia used its influence to help elect Donald Trump, sought to interfere in at least 21 State elections, executed a propaganda campaign to manipulate and sow discord among the American people, and hacked our Nation's critical infrastructure, including U.S. electricity grids.

Since then, President Trump's former National Security Adviser, Michael Flynn, and the President's former campaign policy adviser, George Papadopoulos, both have pleaded guilty to lying to the FBI about their contacts with Russia. President Trump also fired James Comey, the Director of the Federal Bureau of Investigation, because he continued to investigate the "Russia thing" while refusing to pledge his loyalty to President Trump.

Russia's aggression toward the United States and the Trump administration's efforts to cover up its communications with the Russians demand an immediate, whole-of-Government response. Yet, Republican House leaders and Committee Chairmen have blocked, stonewalled, and rejected our basic requests to investigate, hold public hearings, and advance legislation to address these matters. House Republicans have chosen to put President Trump ahead of our National interests.

Rather than pursue the truth on behalf of the American people, House Republicans have waged an aggressive campaign to shut down Congressional and criminal investigations into Russia's attack, they have launched and re-launched investigations into baseless conspiracy theories to deflect attention and resources, they have defamed our Nation's top law enforcement and intelligence agencies, and they have sought to discredit anyone seeking to uncover wrongdoing, including Special Counsel Robert Mueller, a decorated war veteran.

To date, the House has held only one full committee public hearing on the most significant finding of the ODNI report: That our elections continue to be vulnerable to foreign interference in the future. Instead, they have relegated this issue to a handful of toothless subcommittee hearings, which have been marked by the Trump administration's refusal to provide documents requested by Democrats that would help inform our work, such as documents relating to Russia's attempted attacks against 21 State election systems that are currently being withheld by the Department of Homeland Security. Our country, our democracy, and the American public deserve better.

As Members of Congress, we take a solemn oath to support and defend the Constitution and protect the American people. The failure of House Republicans to take strong and swift action in the face of Russia's assault on our democracy is beneath the dignity of this oath. The strength and integrity of our democracy, the rule of law, and our democratic institutions hang in the balance.

We ask you to change course and begin demonstrating true leadership on this critical National security issue. We request that House Republicans join us in fulfilling our sworn Constitutional duty by ensuring that each committee of jurisdiction thoroughly investigates the following key questions:

- How were Russian hackers able to penetrate our State election systems, and how do we protect our elections infrastructure in advance of upcoming elections this year and beyond?
- What vulnerabilities remain in our electrical grids and infrastructure networks, and what can we be doing to ensure our safety and security?
- How was social media leveraged to influence voters, and what can be done to ensure that American voters know where their information is coming from?
- What was the extent of the Trump campaign's involvement in Russia's operation to hack and disseminate material damaging to Hillary Clinton?
- In light of President Trump's refusal to release his tax returns, what is the extent of his and his family's business and financial ties to Russians, and how might those ties constitute leverage over the President and his family?
- In light of Attorney General Jeff Sessions' testimony in October that the Trump administration is not doing enough to stop future Russian interference and that "the matter is so complex that for most of us we are not able to fully grasp the technical dangers that are out there," what steps has the Trump administration taken to hold Russia accountable for its attack and ensure the safety of our elections from foreign interference?
- Why is the Trump administration dragging its feet on implementing the sanctions against Russia that were adopted by Congress with widespread bipartisan support?
- What are the extent and nature of efforts by the Trump administration to impede criminal and Congressional investigations into the Trump campaign's involvement and support for Russian interference into our elections?

We are extremely concerned by the intelligence community's warning that Russia may attempt to interfere with future elections—including the upcoming mid-term elections—and we are deeply troubled by the lack of action by the Trump administration and House Republicans in responding to this core threat to our democracy.

We ask you to review this request and to schedule a meeting with leaders of both parties so we may work together to respond to the matters of serious concern raised in this letter. Thank you for your consideration of these requests.

Sincerely,

CONGRESSMAN ELIOT ENGEL,
Ranking Member of the Foreign Affairs Committee.

CONGRESSWOMAN MAXINE WATERS,
Ranking Member of the Financial Services Committee.

CONGRESSMAN JERROLD NADLER,
Ranking Member of the Judiciary Committee.

CONGRESSMAN BENNIE THOMPSON,
Ranking Member of the Homeland Security Committee.

CONGRESSMAN ELLJAH CUMMINGS,
Ranking Member of the Oversight and Government Reform Committee.

CONGRESSMAN ROBERT BRADY,
Ranking Member of the House Administration Committee.

LETTER FROM RANKING MEMBER BENNIE G. THOMPSON

February 16, 2018.

Chairman MICHAEL T. MCCAUL,
Committee on Homeland Security, H2-476 Ford House Office Building, Washington, DC 20515.

DEAR CHAIRMAN MCCAUL: I am writing to express my continued concern about election security and Russian interference in our election systems. I ask that you to take urgent action by holding a hearing on this important homeland security issue and marking up recently-introduced legislation to protect our election systems, H.R. 5011, the Election Security Act. Both actions should be taken without delay as the first election of the 2018 season will take place in your home State of Texas on March 6, 2018.

In November 2016, 139 million Americans cast their votes in the wake of a massive Russian cyber-enabled influence operation designed to undermine faith in American democracy, exposing serious National security vulnerabilities in our election infrastructure.

In response, on January 6, 2017, then-Secretary of Homeland Security Jeh Johnson designated election infrastructure as a critical infrastructure subsector, citing its importance to our National interests. The same day, the Office of the Director of National Intelligence (ODNI) released a declassified report entitled "Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution" that concluded the Kremlin would use lessons from its 2016 elections operations to influence future elections world-wide. Similarly, in March 2017, during a hearing before the House Permanent Select Committee on Intelligence, then-Federal Bureau of Investigation (FBI) Director James Comey warned that Russia would use its experience from the 2016 elections to attempt to influence upcoming U.S. elections.

Recognizing the alarming conclusions of our National security and intelligence agencies and on-going reports of our foreign adversaries' intentions, on May 23, 2017, I wrote to you to request a Committee on Homeland Security investigation into Russian interference in our elections. While this committee failed to take action, Government officials continued to sound the alarm. At the Aspen Security Forum in July 2017, the Director of National Intelligence, the Director of the Central Intelligence Agency, the former Secretary of Homeland Security, and the White House's Homeland Security Advisor all agreed that Russian entities targeted the 2016 elections. Additionally, in July 2017, a Department of Homeland Security official testified before the Senate Select Committee on Intelligence that State election systems were targeted by nefarious Russian actors. Even after it came to light that almost half of U.S. States had been targeted by the Russians, including States Members of the Committee on Homeland Security call home, our committee did not have a single noticed activity on the issue.

Absent action on my request, on June 29, 2017, I joined with colleagues from the Committee on Homeland Security and the Committee on House Administration to

form the Congressional Task Force on Election Security. Earlier this week, after months of engagement with State election officials, security experts, and other stakeholders, the Task Force released a comprehensive report with findings and recommendations and unveiled the Election Security Act, which is aimed at bolstering protections for upcoming U.S. elections.

The Task Force's report comes on the heels of still more warnings from U.S. Government officials that Russia seeks to interfere with our upcoming elections. Indeed, a week prior to the release of our report, Secretary of State Rex Tillerson stated that Russia is already trying to interfere in the 2018 midterm elections. On February 13, the day prior to the release of the Task Force's final report, 6 current intelligence officials—the Director of National Intelligence, the Director of the Central Intelligence Agency, the Director of the FBI, the Director of the National Security Agency, the Director of the Defense Intelligence Agency, and the Director of the National Geospatial Intelligence Agency—unanimously agreed that the 2018 elections are a potential target for Russian operations.

Given the seriousness of this threat to our Nation, Congress must redouble its efforts to thwart foreign influences seeking to interfere in our elections. The Committee on Homeland Security should have acted long ago. With less than 10 legislative days prior to the first primary election of the year, it is critical that we hold a hearing to examine this National security issue and consider the Election Security Act without delay. We owe it to the American public to act. I look forward to working with you to secure our Nation's elections and our democracy.

Sincerely,

BENNIE G. THOMPSON,
Ranking Member.

LETTER FROM CHAIRMAN MICHAEL T. MCCAUL

February 21, 2018.

Ranking Member BENNIE THOMPSON,
Committee on Homeland Security, H2-117 Ford House Office Building, Washington, DC 20515.

DEAR RANKING MEMBER THOMPSON: Thank you for your February 16, 2018 letter. Russian interference in our electoral process and the undermining of our democratic institutions by a foreign adversary must never be tolerated. That is why I am proud of our bipartisan efforts to pass the first ever, comprehensive reauthorization of the Department of Homeland Security (DHS). Specifically, I am glad we adopted an amendment that prioritizes and requires DHS to provide voluntary assistance to State and local election officials in recognition of the importance of election infrastructure. Not only did we pass this bill unanimously through our committee, it passed through the House with overwhelming bipartisan support last July by a vote of 386–41.

It is imperative that we continue to ensure DHS has the most efficient and robust structure possible to help thwart all cyber adversaries. The bipartisan Cybersecurity and Infrastructure Security Agency Act of 2017, which I introduced and you co-sponsored, elevates and operationalizes the Department's cybersecurity and infrastructure protection offices, helping to ensure stronger mission execution which is so integral to our shared concerns. This bill also sailed through the House with support from both parties. The Senate should follow our lead and get these bills to the President's desk.

While recognizing Russian interference in our election in October of 2016, I called on President Obama to "send a clear signal to Moscow: attempts to influence U.S. elections or interfere with our democratic system will be met with severe consequences." Since that time, I have remained consistent on the seriousness of this threat. Just last week, I called for the extradition of Russians who had been indicted for election interference, so they could be "held accountable and prosecuted to the fullest extent of the law." Clearly, these kinds of attacks transcend partisan politics.

I want to encourage all Members of the committee to raise this vital issue when Secretary Nielsen appears before the committee during our March budget hearing. In addition, it is my goal to have the Under Secretary of the National Protection and Programs Directorate, once confirmed, appear before the committee to discuss this, and other key cyber issues, in classified and unclassified settings.

I look forward to working with you to protect the integrity and transparency of our American democracy.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

LETTER FROM FIFTEEN MEMBERS OF CONGRESS

March 6, 2018.

The Honorable RODNEY P. FRELINGHUYSEN,
*Chairman, Committee on Appropriations, U.S. House of Representatives, Wash-
 ington, DC 20151.*

The Honorable NITA M. LOWEY,
*Ranking Member, Committee on Appropriations, U.S. House of Representatives
 Washington, DC 20515.*

The Honorable TOM GRAVES,
*Chairman, Subcommittee on Financial Services and General Government, Committee
 on Appropriations, U.S. House of Representatives, Washington, DC 20515.*

The Honorable MIKE QUIGLEY,
*Ranking Member, Subcommittee on Financial Services and General Government,
 Committee on Appropriations, U.S. House of Representatives, Washington, DC
 20515.*

DEAR CHAIRMAN FRELINGHUYSEN, CHAIRMAN GRAVES, RANKING MEMBER LOWEY,
 AND RANKING MEMBER QUIGLEY: We write to express strong support for the Election
 Assistance Commission (EAC), and to respectfully request that the EAC receive \$14
 million so it can continue to assist States in their urgent efforts to secure voting
 systems in advance of the 2018 midterm elections. In addition, we request that you
 appropriate \$400 million under the Help America Vote Act of 2002 (HAVA) for
 States to use to replace aging and vulnerable voting machines and to provide cyber-
 security training.¹ Intelligence officials continue to warn that our State-based elec-
 toral system is a target for foreign meddling and cyber attacking, and we believe
 this money is necessary to protect American elections against the possibility of im-
 minent attack.²

The EAC is the only Federal agency charged with making American elections
 more secure, accessible, accurate, and transparent. It has built strong relationships
 with State and local election officials as well as cybersecurity experts, and has been
 vital to helping States understand and respond to the threats confronting their elec-
 tion infrastructure. The EAC has worked diligently, with a bare-bones budget, over
 the past few years to provide guidance on cybersecurity and election technology. But
 at this critical time, the Commission needs additional resources to fully respond to
 the needs of the States.

Providing the EAC with additional funds would enable them to hire two addi-
 tional staffers whose exclusive responsibilities would be to work directly with State
 and local election officials, as well as cybersecurity experts, on improving cybersecu-
 rity. In addition, the agency could hire two additional researchers to develop best
 practices on cybersecurity and risk-limiting audits, and to create materials to train
 election officials and poll workers on security issues. The EAC would also be able
 to hold a summit to bring together computer scientists, “white hat” hackers, and
 academics to examine election technologies and expose any vulnerabilities before the
 equipment is put to use. Finally, the EAC could increase the amount of funds it
 transfers to the National Institute of Standards and Technology (NIST) to \$2.5 mil-
 lion which would enable NIST to provide further technical expertise on voting ma-
 chine standards.

Furthermore, States need an additional \$400 million in grants under HAVA to be
 appropriated so they can safeguard their voting infrastructure. The single most ur-
 gent need is for States using paperless machines to replace their outdated equip-
 ment with paper ballot voting systems. The Brennan Center estimates that the cost
 to replace paperless voting machines is between \$130 and \$400 million, and States
 do not have the money to do it themselves.³ Moreover, State and local officials have
 expressed a desire for Congress to step in. In December 2017, the National Associa-
 tion of Secretaries of States (NASS) called upon Congress to provide the States with
 the remaining HAVA funds. President of NASS and Indiana Secretary of State

¹ Pub. L. 107–252 (Oct. 29, 2002).

² Ellen Nakashima and Shane Harris, “The Nation’s Top Spies Said Russia is Continuing to
 Target the U.S. Political System,” *Washington Post* (Feb. 13, 2018) available at [https://
 www.washingtonpost.com/world/national-security/tbi-director-to-face-questions-on-security-
 clearances-and-agents-independence/2018/02/13/f3e4c706-105f-11-e8-9570-29c9830535e5_story.html?utm_term=.9f97e032916c](https://www.washingtonpost.com/world/national-security/tbi-director-to-face-questions-on-security-clearances-and-agents-independence/2018/02/13/f3e4c706-105f-11-e8-9570-29c9830535e5_story.html?utm_term=.9f97e032916c).

³ Lawrence Norden and Ian Vandewalker, “Securing Elections From Foreign Interference,”
Brennan Center (June 29, 2017), available at <https://www.brennancenter.org/publication/securing-elections-foreign-interference>.

Connie Lawson said, “The challenges faced by State and local election officials in 2017 are quite different from those we faced in 2002.”⁴

Appropriating a new round of HAVA grants would not address all security concerns. As you may know, the Congressional Task Force on Election Security found that States need funding to hire IT staff, upgrade and maintain IT infrastructure, implement risk limiting audits, develop more secure election technology, and for cybersecurity training. Toward that end, its legislative proposal requests a total of \$1.8 billion—half of the amount initially authorized to fight hanging chads in HAVA—over 10 years to replace all non-secure voting machines, maintain and upgrade elections systems, provide on-going cybersecurity training, help States implement risk limiting audits, and invest in innovative election technology. But the \$400 million already authorized would allow States to address their biggest vulnerability by replacing paperless voting machines and would represent an important down payment on tackling this long-term National security challenge.

We cannot leave States to their own devices in defending against the sophisticated cyber tactics of foreign governments. An attack on the electoral infrastructure in one State is an attack on all of democracy in America. Michael Chertoff, former Secretary of Homeland Security, and Grover Norquist wrote in *The Washington Post*, “It’s not practical to expect local election administrators in rural Missouri or small-town Maine to go toe-to-toe with the premier government-backed cyber mercenaries in China or North Korea. Just as Federal agencies prudently provide support for State law enforcement in dealing with terrorism, Federal officials should give guidance and support in dealing with the election cybersecurity threat.”

We urge you to fully fund HAVA and provide the EAC with the support it needs so that the Federal Government can meaningfully assist States in securing our election systems.

Thank you for your attention to this important matter.

Very truly yours,

STENY HOYER,
Member of Congress.

ROBERT A. BRADY,
Member of Congress.

ZOE LOFGREN,
Member of Congress.

JAMIE RASKIN,
Member of Congress.

BENNIE G. THOMPSON,
Member of Congress.

LISA BLUNT ROCHESTER,
Member of Congress.

JOAQUIN CASTRO,
Member of Congress.

JIM COOPER,
Member of Congress.

VAL DEMINGS,
Member of Congress.

JAMES R. LANGEVIN,
Member of Congress.

JOHN LEWIS,
Member of Congress.

DONALD M. PAYNE,
Member of Congress.

BRAD SCHNEIDER,
Member of Congress.

JOHN YARMUTH,
Member of Congress.

CEDRIC L. RICHMOND,
Member of Congress.

⁴National Association of Secretaries of States. (December 15, 2017). *NASS Calls on Congress to Provide the Remaining \$396 Million in Outstanding HAVA Funds*. [Press release].

LETTER FROM RANKING MEMBER BENNIE G. THOMPSON

March 12, 2018.

The Honorable MICHAEL T. MCCAUL,
Chairman, Committee on Homeland Security, Washington, DC 20515.

DEAR MR. CHAIRMAN: I am pleased that on Wednesday, March 7, you publicly announced that the committee would commence efforts to address two homeland security issues—election security and school security. On the subject of election security, I was pleased to hear you express that you share concerns that I, along with my Democratic colleagues on the committee, have repeatedly expressed about the prospect that Vladimir Putin’s cyber hackers continue to pose a threat to our election infrastructure and that the 2018 elections are a target. Further, you informed the committee that on March 6 you sent a request for a Classified briefing from the Department of Homeland Security (DHS) on the cybersecurity threats facing State election systems. I request that this Classified briefing be an official noticed activity. You also indicated that you intend to notice a public hearing dedicated to receiving testimony on election security from Federal Government witnesses as soon as possible. There are just 8 legislative days left until the next Congressional work period. As such, I would appreciate information on the projected time line for holding both the election security briefing and hearing.

With respect to school security, I was heartened to hear you acknowledge that school security is a homeland security issue. I was also pleased to hear you express interest to move forward, on a bipartisan basis, with school security legislation in this committee. However, I am disappointed that consideration of H.R. 4627, the “Shielding Public Spaces from Vehicular Terrorism Act” was postponed. As such, a timely amendment Rep. Val Demings (D-FL) authored, addressing the risk that President Trump could direct DHS to abandon a long-standing prohibition on Federal homeland security grant expenditures on guns to allow such purchases for teachers, did not get considered. While I was pleased to hear you acknowledge that this prohibition is a long-standing DHS policy, I was perplexed to learn that the Majority needs more time to seek more information to “properly vet” the amendment, given that no outreach was made to Rep. Demings or my staff since Monday, March 5 at 10 a.m., when the amendment was filed as required under the committee notice. Action on the Demings legislation is necessary, given that the President recently expressed support for Federal funding to be provided to cover firearms training for K–12 educators.

We would welcome the opportunity to work on a bipartisan basis to make our Nation’s schools more secure to terrorism, active shootings, and other threats, as you expressed was your goal. We stand ready to work with you on such legislation, and we would appreciate greater detail when you expect to take up H.R. 4627 with concern to your goals, timing-wise, for bipartisan school security legislation.

Further, I believe the bipartisan school security legislative effort could be bolstered by the committee holding a hearing outside of the Capitol. To that end, I would highlight that on March 6, Emergency Preparedness, Response, and Communications (EPRC) Ranking Member, Donald M. Payne, Jr. (D-NJ), submitted a request for a field hearing to conduct oversight on DHS’s effort to improve school security and preparedness in his New Jersey Congressional district. As you know, Ranking Member Payne’s interest in this homeland security issue dates back to 2013, when he introduced the “SAFE in Our Schools Act” (H.R. 3158).

Election security and school security demand urgent action. Accordingly, I look forward to getting a more detailed picture of your specific plans for committee action on these homeland security challenges, as sought above. Together, I believe we can, in a bipartisan way, make our children, constituents, communities, and this democracy more secure.

To coordinate such effort, please do not hesitate to have your staff contact my staff director, Hope Goins.

Thank you.

BENNIE G. THOMPSON,
Ranking Member.

IN THE NEWS—KEEPING THE VOTE CYBERSAFE

AUG 13, 2016, *The New York Times*

To the Editor:

In “U.S. Seeking Ways to Keep Hackers Out of Ballot Box” (news article, Aug. 4), Homeland Security Secretary Jeh Johnson says the Obama administration is dis-

cussing giving extra protections to the Nation's electoral system. This change may be necessary and should be considered immediately.

The diverse nature of the cyber threat, and the recent revelation that outside actors, possibly nation-states, have an increased interest in influencing our elections, make it imperative that the Federal Government give additional attention to securing our electoral system and possibly deem it part of our Nation's critical infrastructure.

Without delay, Mr. Johnson should communicate with the thousands of jurisdictions in the country that help carry out elections and offer the Department of Homeland Security's assistance, expertise, and guidance. While the diverse and varied nature of our voting infrastructure confounds efforts to secure it, this tells us that the process should begin as soon as possible.

PRESS RELEASE—THOMPSON, SMITH, CUMMINGS, CONYERS, ENGEL, HOYER, SCHIFF
JOINT STATEMENT CALLING FOR A COMPREHENSIVE INVESTIGATION OF RUSSIAN INTERFERENCE IN THE 2016 ELECTION

DEC. 13, 2016

(WASHINGTON).—Today, House Armed Services Committee Ranking Member Adam Smith (D-WA), House Oversight Committee Ranking Member Elijah Cummings (D-MD), House Judiciary Committee Ranking Member John Conyers (D-MI), House Foreign Affairs Committee Ranking Member Eliot Engel (D-NY), House Democratic Whip Steny Hoyer (D-MD), House Intelligence Committee Ranking Member Adam Schiff (D-CA), and Homeland Security Committee Ranking Member Bennie G. Thompson (D-MS) released the following joint statement in response to news reports about intelligence assessments of Russian interference in the 2016 election, and comments by the House Republican leadership downplaying the need for a thorough investigation:

"All Americans should be deeply concerned by the reports that Russian agencies have interfered with a U.S. election. As Speaker Ryan noted, 'any foreign intervention in our elections is entirely unacceptable.'

"The first duty of the United States Government is to safeguard the American people and the integrity of our free society from attacks by foreign adversaries. Cyber attacks on our political institutions are direct threats to their integrity and are just as menacing as attacks on our economic, physical, and military infrastructure.

"Given the gravity of these unprecedented attacks by a foreign state, we need a Congressional investigation that is truly bipartisan, that is comprehensive, that will not be restricted by jurisdictional lines, and that will give the American people a complete and full accounting of what happened consistent with safeguarding our National security."

PRESS RELEASE—CONGRESS MUST PROTECT ELECTORAL SYSTEMS & PRESERVE
ELECTION ASSISTANCE COMMISSION

DHS PROMISES TO HELP STATES PROTECT SYSTEMS AS HOUSE GOP VOTES TO ELIMINATE
COMMISSION

FEB. 8, 2017

(WASHINGTON).—Yesterday, the Committee on House Administration voted on party lines to eliminate the independent Election Assistance Commission. The EAC was created to help States upgrade voting technology and promote critical election-related information sharing. Having up-to-date voting machine technology is critical to ensure they are protected from any potential hacking, tampering, or fraud.

This inexplicable move willfully ignores the present-day threats to election infrastructure. In fact, yesterday, Homeland Security Secretary John Kelly stated to Congress: "I believe we should help all of the States, provide them as much help as we can to make sure their systems are protected in future elections" [VIDEO of exchange with Rep. Cedric Richmond]. He also noted that protecting the Nation's electoral systems should be a priority under the National Infrastructure Protection Plan. Additionally, President Trump has said that our election systems were compromised in the 2016 election and millions illegitimately voted. Those allegations are reported to be investigated by the White House under a commission that lacks the independence of the EAC.

Rep. Bennie G. Thompson (D-MS), Ranking Member of the Homeland Security Committee, released the following statement on the change:

“The danger of cyber attacks from state and non-state actors is constantly escalating and evolving and Americans must be confident that we are addressing this threat. Congress cannot abdicate this responsibility while the President sends Federal investigators on a wild goose chase to search for millions and millions of non-existent illegal votes. Given public unease regarding Russia’s extensive interference with the recent Presidential election, Congress should be doing more, not less, to ensure the integrity of our electoral systems. Our legitimacy as Congress is only as legitimate as strength and security of the ballot box. This is a shameful, partisan move by House Republicans that undermines our democracy.”

Rep. Cedric L. Richmond (D-LA), Ranking Member of the Subcommittee on Cybersecurity and Infrastructure Protection, added the following:

“Voting is a fundamental right and the foundation of our democracy and it is essential that we maintain confidence in the integrity of the ballot box. Now that constant cyber attacks are our new reality, taking the appropriate security measures is more important than ever. If we are serious about protecting our electoral process we need to continue to make smart investments like the EAC that will help us reach that goal.”

IN THE NEWS—INDEPENDENT COMMISSION MUST INVESTIGATE PRESIDENT TRUMP’S
POTENTIAL RUSSIAN TIES

FEB. 27, 2017, *BlackPressUSA*

The endurance of our Nation’s security, sovereignty, and democracy is not a partisan issue. This is a top concern for all Americans and should be a top priority for the leaders that we send to Washington, whether Democrat or Republican. As elected officials, my colleagues and I swore to support and defend the Constitution of the United States against all enemies, foreign and domestic. We, therefore, have a responsibility to do our due diligence in investigating Russian interference, and potential influence, into our democratic elections and the potential Russian on-going connections within this current Presidential administration.

Despite all of the evidence gathered thus far—evidence that has led all 17 of the U.S. intelligence agencies to conclude with confidence that the Russians had indeed interfered in the past election—the current administration seems unable or unwilling to put its full weight behind a full and proper investigation that seems necessary to the American people. In the face of evidence that campaign and administration officials seem to have had relationships with Russian officials, the President cannot simply move on from this issue. In fact, the resignation of National Security Advisor Michael Flynn this month seems to provide us with more questions than answers.

The potential conflicts between the Trump administration and its apparent ties to Russia seem numerous. The President has refused to release his tax returns—a move not seen from any other modern major party candidate—leaving questions unanswered as to potential Russian business ties and conflicts of interest that President Trump was all too happy to gloat about in years past. The President is unable to criticize Russia and its dictator-like leader Vladimir Putin, but, instead, praises him and prefers him to President Obama. When confronted with the assertion that Putin has had journalists and political opponents killed, President Trump doubled down on his support of Putin by shockingly asserting a moral equivalence between Russia and the United States.

The President’s ties to Russia don’t end with him, however, they trickle down into his administration. As in the campaign, President Trump continues to surround himself with advisers that have expansive and well-documented financial entanglements to Russia. Recently, *The New York Times* reported that phone records show Trump associates communicated with senior Russian intelligence officials throughout the campaign, including his former campaign chair Paul Manafort, who is known to have involvements in multimillion-dollar business deals with Putin allies in Ukraine. Additionally, Michael Flynn was forced to resign following information revealing that he had lied about privately discussing U.S. sanctions against Russia with the Russian ambassador to the United States before Trump took office, a potentially illegal act. It has since been reported that White House officials were made aware of Flynn’s actions and made no effort to correct the record. It was only after leaks to the public that President Trump’s hand was forced, raising concerns regard-

ing the ability of this White House to maintain honest and open communication with the American people.

This intricate web leaves us with critical questions that must be answered. What did the President know and when? Was the White House ignoring or covering up the truth and spreading misinformation? Did Flynn operate at the direction or the knowledge of the President and were others involved? The American people deserve to know the full extent of Russia's financial, personal, and political strings attached to President Trump and this administration.

Now more than ever, we need an independent, bipartisan commission to fully investigate Russia's interference in the election and any potential Trump campaign ties to the Kremlin. Unfortunately, Republican leaders in the House seem less than enthusiastic about investigating their own President. In turn, last month, Representatives Eric Swalwell (D-CA), and Elijah Cummings (D-MD) reintroduced legislation that would create a 12-member, bipartisan, independent commission empowered to conduct an in-depth investigation into attempts by the Russian government or others to use electronic means to influence, interfere with, or undermine trust in last year's elections. This would be similar to the highly-praised 9/11 Commission—which was led by well-regarded National security experts that were not elected officials. Such a commission is not only necessary in order to ensure our security, but to restore trust in this administration and in the democratic process. All Democratic Members of the House of Representatives, along with one Republican, have co-sponsored this critical bipartisan legislation.

The American people deserve transparency and peace of mind when it comes to their elected leadership. The Trump administration has insisted on remaining friendly with Russia despite the very clear threat that they have presented to our National security. In doing so, they have put our Nation at risk while keeping American citizens in the dark. The Trump administration's intent to ignore these on-going acts of aggression sends a message that this type of meddling is acceptable. The only democratic way forward is to launch a complete investigation into not only the interference into our democratic election, but also into the ties and communication that this administration has had with Russia.

PRESS RELEASE—AG SESSIONS MUST PRIORITIZE ELECTION HACKING INVESTIGATION
AFTER YAHOO INDICTMENTS

MARCH 15, 2017

(WASHINGTON).—Today, Rep. Bennie G. Thompson (D-MS), Ranking Member of the Committee on Homeland Security, released the following statement on news that the Justice Department announced the indictments of two Russian spies and two criminal hackers in connection with the 2014 hack of Yahoo.

"Today's Justice Department indictment of two Russian-government agents in the Kremlin's cyber division is a watershed moment in our efforts to counter state-directed cyber hacking campaigns. Without doubt, the tactics utilized in the Yahoo plot are a roadmap to how the Kremlin carries out its cyber hacking campaigns. I call on Attorney General Sessions to prioritize the investigation of the cyber hacking campaign against our political institutions during the 2016 election with an eye to indicting whoever in Vladimir Putin's government directed this unprecedented attack on our democracy."

PRESS RELEASE—PELOSI, THOMPSON, BRADY ANNOUNCE ELECTION SECURITY TASK
FORCE

JUNE 29, 2017

(WASHINGTON).—Today, as the Nation prepares to celebrate July 4th, House Democratic Leader Nancy Pelosi, Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS), and Committee on House Administration Ranking Member Robert Brady (D-PA) announced the formation of a Task Force to ensure the health and security of our Nation's election systems.

The Congressional Task Force on Election Security will address the lack of action to protect electoral infrastructure following Russia interfering and attempting to influence the 2016 Presidential election. According to the Department of Homeland Security, the election systems in 21 States were breached and voter records containing personal information were stolen. To this day, we have seen no action from

the Republican Congress or the Trump administration to provide greater protection to our election systems.

The Congressional Task Force on Election Security is intended to be a forum for Members from the two committees to hear from experts with expertise in cybersecurity and election infrastructure and identify policy recommendations that can help ensure the integrity of our election systems and guard against future attacks.

Leader Pelosi released the following statement on the Task Force:

“The integrity of our democracy itself is under threat from the Russians,” said House Democratic Leader Nancy Pelosi. “But we see an appalling absence of action, or even concern, from President Trump and Congressional Republicans. Democrats won’t allow Putin’s assault on American democracy to go unchallenged. With our Task Force on Election Security, House Democrats are continuing to pursue the facts and defend our democracy where Republicans won’t.”

Ranking Member Thompson added the following:

“Last year’s Russian campaign to hack our political institutions and interfere with the Presidential election was a blatant attack on our democracy. If we continue to do nothing to protect the integrity of our election systems, we make it easy for Russia and other nefarious actors to impact future elections. Unfortunately, we have seen no effort from the Republican-led Congress or the Trump administration to address this vulnerability. Looking toward the future, we must be able to put politics aside for the good of the country and work together to protect against efforts to undermine our cherished democratic institutions. I look forward to working with Ranking Member Brady and my colleagues to get answers for the American people and prevent future damage to our democracy.”

Ranking Member Brady added the following:

“We now know that Russia launched an unprecedented attack on our election infrastructure, and the intelligence community has indicated that foreign actors will be back in 2018 and 2020. Free, fair, and secure elections are the cornerstone of our democracy, and Congress must take action to address this threat to our election security, and our National security. I look forward to working with my colleagues to identify the vulnerabilities in our voting systems and to take action to make our elections safer.”

PRESS RELEASE—ELECTION SECURITY TASK FORCE RECEIVES FIRST BRIEFING

JULY 27, 2017

(WASHINGTON).—The Congressional Task Force on Election Security, chaired by Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) and Committee on House Administration Ranking Member Robert Brady (D-PA) received its first information-gathering briefing to inform its work on securing our election systems.

The Task Force was briefed by the Brennan Center For Justice on its new report: *Securing Elections From Foreign Interference*. Brennan Center experts offered specific actions Congress and local election officials can quickly take to insulate voting technology from continued foreign interference. Their report focuses on assessing and securing two of the most vulnerable points in the system: voting machines, which could be hacked to cast doubt on or change vote totals; and voter registration databases, which could be manipulated in an attempt to block voters, cause disruption, and undermine confidence when citizens vote.

Co-Chairs Thompson and Brady released the below joint statement following the briefing:

“Russia’s meddling in the 2016 election and targeting of voting infrastructure in at least 21 States was a direct attack on our democracy. The American people expect their Government to do whatever possible to prevent this from happening again. While Republicans refuse to look into this issue, we are taking the steps to begin an investigation into what we can do to secure our election infrastructure and prevent what transpired last year from happening again. The Brennan Center’s expertise on election issues will lend us to our first public meeting in the coming weeks where we will hear from officials and experts with diverse backgrounds. This will be the first step toward forming solutions to protect our democracy and its cherished institutions from malicious actors and outside influence.”

PRESS RELEASE—THOMPSON STATEMENT ON DHS NOTIFYING STATES OF ELECTION
TARGETING

SEPTEMBER 22, 2017

(WASHINGTON).—Today, Rep. Bennie G. Thompson (D-MS), Ranking Member of the Committee on Homeland Security, released the following statement on the news that the Department of Homeland Security (DHS) has notified each State and territory whether or not their election systems were targeted during the 2016 election:

“Russia’s priority in undermining confidence in our democratic institutions was clear during last year election and will only growing stronger. To counter this, there must be a strong relationship between DHS and its partners at the State level with the aim of keeping our election systems—part of our critical infrastructure—secure. While this should have happened much sooner, I am glad that DHS finally notified each State whether or not they were targeted by Russia. I urge DHS to keep building trusted relationships with State governments to carry out its responsibility to help States secure their election systems. Congress must also continue to do its part to investigate what happened last year, work to prevent it in the future, and ensure DHS has the resources it needs to protect these systems.”

PRESS RELEASE—UPDATED: ELECTION SECURITY TASK FORCE TO HOLD FIRST
PUBLIC FORUM THURSDAY

SEPTEMBER 26, 2017/SEPTEMBER 27, 2017

(WASHINGTON).—On Thursday, September 28th, the Congressional Task Force on Election Security, will hold its first public forum: “Securing America’s Elections: Understanding the Threat.” The task force will hear from Jeh Johnson, former Homeland Security Secretary, and Suzanne Spaulding, former DHS Under Secretary for the National Protection and Programs Directorate.

Details: Congressional Task Force on Election Security Forum “Securing America’s Elections: Understanding the Threat” 11 a.m. Thursday, September 28th Location: 1302 Longworth House Office Building ***NOTE ROOM CHANGE***.

The Congressional Task Force on Election Security was created this summer to address the lack of action to protect electoral infrastructure following Russia interfering and attempting to influence the 2016 Presidential election. It is chaired by Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) and Committee on House Administration Ranking Member Robert Brady (D-PA).

Co-Chairs Thompson and Brady released the below joint statement announcing the forum:

“Recent news reminds us that Russia targeted voting infrastructure in at least 21 States last year in a direct attack on our democracy. Looking forward, the American people expect us to investigate our vulnerabilities and do whatever possible to prevent this from happening again. While Republican leaders in Congress refuse to investigate, we have decided to take initiative to start a process to provide answers on how we can better secure our election infrastructure and prevent election meddling in the future.”

PRESS RELEASE—ELECTION SECURITY TASK FORCE RELEASES PRELIMINARY
RECOMMENDATIONS

NOVEMBER 15, 2017

(WASHINGTON).—The Congressional Task Force on Election Security, chaired by Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) and Committee on House Administration Ranking Member Robert Brady (D-PA) released its preliminary findings and recommendations marking 1 year since the 2016 election. Because of Republican inaction, the Task Force was created this summer to put forth solutions to secure our election systems after Russia interfered and attempted to influence last year’s election. Just yesterday, Attorney General Jeff Sessions admitted to Congress that he could not report on any administration election security efforts.

Over the past 5 months, the Task Force has held public forums with election and cybersecurity experts and has been working to understand the threats to election infrastructure and how to address them. The 5 findings and 6 recommendations re-

leased today underline the Department of Homeland Security and the Election Assistance Commission as the primary agencies that can help States better secure their election systems. Today's preliminary findings will inform an upcoming final task force report.

Preliminary recommendations:

- Maintain the designation of election infrastructure as a critical infrastructure subsector.
- Help States fund and maintain secure election systems.
- States should conduct post-election risk-limiting audits.
- Empower Federal agencies to be effective partners for Nation-wide security reforms.
- Establish clear and effective channels for sharing threat and intelligence information with election officials.
- Prioritize cybersecurity training at the State and local level.

Congressman Thompson and Congressman Brady released the following statement:

"One year ago, 139 million Americans cast their vote in the wake of a massive Russian cyber-enabled influence operation designed to undermine confidence in our democracy. Russia also targeted voter registration databases in at least 21 States and sought to infiltrate the networks of voting equipment vendors, political parties, and at least one local election board. If we do nothing, this will become our new normal. With the next Federal election only 1 year away, it is high time we start thinking about enacting real solutions. The findings and recommendations released today are an outline of concrete steps that we can take to ensure our elections are more secure going forward."

PRESS RELEASE—PELOSI, RANKING MEMBERS TO HOLD PRESS CONFERENCE ON HOUSE REPUBLICANS' INACTION TO SUFFICIENTLY INVESTIGATE RUSSIA'S THREAT TO OUR DEMOCRACY

JANUARY 8, 2018

(WASHINGTON).—House Democratic Leader Nancy Pelosi, Ranking Members Eliot Engel, Maxine Waters, Jerry Nadler, and Bennie Thompson, as well as Vice Ranking Member Gerry Connolly will hold a press conference tomorrow at 2:30 p.m. E.T. to highlight House Republicans' inaction to sufficiently investigate and address Russia's threat to our democracy and National security. This press conference comes as we mark 1 year since the Office of the Director of National Intelligence's report confirming Russia's interference into the 2016 election and that our elections continue to be vulnerable to future foreign interference.

- House Democratic Leader Nancy Pelosi
- Congressman Eliot Engel, Ranking Member of the Foreign Affairs Committee
- Congresswoman Maxine Waters, Ranking Member of the Financial Services Committee
- Congressman Jerry Nadler, Ranking Member of the Judiciary Committee
- Congressman Bennie Thompson, Ranking Member of the Homeland Security Committee
- Congressman Gerry Connolly, Vice Ranking Member of the Oversight and Government Reform Committee

Press Conference on House Republicans' Inaction to Sufficiently Investigate Russia's Threat to Our Democracy

Tuesday, January 9, 2018, 2:30 p.m. E.T.

- Radio/TV Gallery Studio A
- Capitol Visitor Center
- The Capitol
- Washington, DC.

This media availability is for Congressionally-accredited media only.

PRESS RELEASE—ELECTION SECURITY TASK FORCE SEEKS CLARIFICATION ON DHS ROLE IN CONTINUING KOBACH VOTER FRAUD COMMISSION

JANUARY 23, 2018

Despite no evidence of voter fraud, President Trump ordered DHS to examine non-existent Commission findings and "determine next course of action"

(WASHINGTON).—Today, House Homeland Security Committee Ranking Member Bennie G. Thompson (D–MS) and Committee on House Administration Ranking Member Robert A. Brady (D–PA), Co-Chairs of the Congressional Task Force on Election Security, wrote to Department of Homeland Security (DHS) Secretary Kristjen Nielsen seeking clarification regarding the Department’s responsibilities related to the now-defunct Presidential Commission on Election Integrity.

The Commission was ostensibly established to investigate allegations of fraudulent voter registrations and fraudulent voting. However, the Members write this claim was substantiated by “nothing more than the President’s active imagination and frustration that he did not receive the majority of the popular votes cast in the 2016 Presidential election.” The letter notes the Commission was the subject of frequent criticism and legal action “alleging violation of several Federal laws, including the Fifth Amendment to the U.S. Constitution, the Privacy Act, the Hatch Act, and multiple State laws, among other things.”

After the commission was unable to produce any evidence of improper voting and registrations, the President abruptly terminated the commission. However, he nevertheless directed DHS to “examine” the Commission’s initial findings and “determine the next courses of action.”

The Members write:

“It is unclear how the Department will carry out this charge given that the Commission never produced any findings. We are concerned that directing DHS essentially to take over where the Commission left off could distract the Department from its pressing obligation to protect U.S. election systems from foreign interference and may undermine the burgeoning relationships DHS is building with State election officials.”

The Members request that DHS provide the following information related to their examination:

- Any documents, files, electronic records, or information that the Department has received or anticipates receiving from the Commission, despite reports that all voter data will be destroyed and that the Commission never made any findings.
- What activities the Department will undertake pursuant to the President’s decision to transfer the Commission’s responsibilities to DHS, including whether those additional activities will require the Department to divert resources from existing activities.
- What steps the Department plans to take in order to avoid undermining the cooperative relationship between DHS and the States necessary to secure our Nation’s elections.

PRESS RELEASE—ELECTION SECURITY TASK FORCE CHAIRS RELEASE STATEMENT ON SECRETARY TILLERSON COMMENTS ON RUSSIA ALREADY INTERFERING IN THIS YEAR’S ELECTIONS

FEBRUARY 8, 2018

(WASHINGTON).—Today, House Homeland Security Committee Ranking Member Bennie G. Thompson (D–MS) and Committee on House Administration Ranking Member Robert A. Brady (D–PA), Co-Chairs of the Congressional Task Force on Election Security, released the below joint statement in reaction to Secretary of State Tillerson’s comments on Russia already interfering in this year’s elections.

“Secretary Tillerson confirmed what Congressional Democrats have known since the ODNI released its report on election meddling: Russia is determined to interfere in our elections and disrupt our democratic processes. His candid admission that we are no better prepared to stop them than we were in 2016 is a testament to President Trump’s failure to acknowledge that Russia interfered in our elections once and is determined to do so again. His unwillingness to counter the threat should be appalling to all concerned Americans.”

“While Republicans in Congress have turned a blind eye, the Trump administration seems to do Putin’s bidding. Congressional Democrats, however, have spent the last year identifying vulnerabilities in our election systems and figuring out what we need to do to secure them. Next week, the Congressional Task Force on Election Security, which we chair, will be releasing its final report, recommendations, and new legislation to give our elections systems a much-needed update.”

“Congress fought hard to protect the integrity of elections against hanging chads 15 years ago, and certainly we should act to protect our elections from the Russian gov-

ernment today. It's time for Republicans to wake up and join us in protecting our democracy from Putin."

The Election Security Task Force wrote the House Appropriations Committee last November stressing the need to appropriate the remaining \$400 million already authorized for election infrastructure under the Help America Vote Act for States to use to help secure their elections systems.

PRESS RELEASE—BRADY, THOMPSON: TRUMP ABDICATING HIS OATH OF OFFICE BY
REFUSING TO ACT ON ELECTION SECURITY

FEBRUARY 27, 2018

(WASHINGTON).—Today, the Co-Chairs of the Congressional Task Force on Election Security, House Homeland Security Committee Ranking Member Bennie G. Thompson (D-MS) and Committee on House Administration Ranking Member Robert A. Brady (D-PA), released the below joint statement on the need for election security measures following Admiral Mike Rogers' testimony before the Senate Armed Services Committee today. At the hearing, the National Security Agency (NSA) Director and U.S. Cyber Command Commander told Senators that President Trump has not given him orders to counter Russian interference in our elections.

"It is unimaginable that the President of the United States has not ordered NSA Director Rogers—or apparently the heads of any other agency—to stop Russia from meddling in our elections. This is a clear invitation for Putin to continue to do what he pleases with American sovereignty and our democratic institutions. Let us be clear: This inaction is the President abdicating his oath of office. While spending time on Twitter falsely alleging a witch hunt, he is not keeping the country safe and secure.

"With a President unwilling or unable to put the country and its security first, Congress must act. We call on Republicans and Democrats to come together and pass clearly-needed election security reforms. The Congressional Task Force on Election Security introduced legislation earlier this month—H.R. 5011, the Election Security Act—that would provide assistance to States to help secure their elections systems and protect our democratic institutions from Russian efforts to undermine them. We hope that our Republican colleagues can join us and put politics aside so we secure our elections—the hallmark of our democracy—from Russian interference."

PRESS RELEASE—HOUSE DEMOCRATS CALL ON REPUBLICAN CONGRESS TO UPHOLD
THEIR OATH OF OFFICE & PROTECT ELECTIONS FROM RUSSIAN ATTACKS

MARCH 6, 2018

(WASHINGTON).—Today, March 6—at the start of the 2018 election season—House Democrats are holding a press conference to release a new letter to the Appropriations Committee Republican leadership calling for necessary funds to protect our Nation's on-going elections from the threat of repeated Russian attacks.

It has been over a year since Russia's unprecedented assault on the country's elections in 2016—including targeting 21 States' voting systems. These attacks exposed serious National security vulnerabilities to our election infrastructure—which includes voting machines and voter registration databases. Since that time, the Trump administration and Republican leadership in Congress—despite their oath of office to protect against enemies foreign and domestic—have refused to address the issue or put forth any solutions to close these security gaps, inviting Russia to interfere in our elections again.

Who:

- Democratic Whip Steny H. Hoyer (D-Md.)
- Rep. Zoe Lofgren (D-Calif.)
- Rep. James R. Langevin (D-R.I.)
- Rep. Jamie Raskin (D-Md.)
- Rep. Joaquin Castro (D-Texas)
- Rep. Brad Schneider (D-Ill.)

What: Press Conference on Election Security

When: Tuesday, March 6, 2018, 1:30 pm ET

Where:

- Radio/TV Gallery Studio B
- Capitol Visitor Center
- The Capitol

- Washington, DC.

NOTE: Press conference is for Congressionally-accredited media only.

PRESS RELEASE—THOMPSON DEMANDS ELECTION SECURITY HEARINGS AFTER
HOMELAND SECURITY CHAIRMAN BACKTRACKS

MARCH 21, 2018

(WASHINGTON).—Today, Rep. Bennie G. Thompson (D-MS), Ranking Member of the House Committee on Homeland Security, released the following statement after receiving written notice from Committee Chairman Michael McCaul (R-TX) that he will not convene a hearing dedicated to election security as he indicated publicly on March 7. While promising to work with Democrats on this issue as soon as possible, Chairman McCaul said: “I look forward to working with you to conducting a full hearing on this issue as it not only impacted—was a real event in the last Presidential election—but I believe it will be a real event in the mid-term 2018 elections.” Today, Homeland Security Secretary Kirstjen Nielsen testified before the Senate Intelligence Committee that our elections are “clearly potential targets for Russian hacking attempts.”

“I am extremely disappointed that Chairman McCaul has already backtracked on his public promise to hold a much-needed hearing on election security and the ongoing Russia cyber threat. This also comes after repeated overtures last year to work together on this issue. Alas, we have made no progress. To be clear, we first began hearing of Russia’s interference in our elections almost 2 years ago.”

“Chairman McCaul often reiterates his opposition to Russia, but actions speak louder than words. Like Speaker Ryan and his fellow House Chairmen, he is ensuring the House stays true in its partisanship and seems too willing to do President Trump’s bidding. Homeland security used to be a bipartisan issue, but it seems this is no longer possible when one party refuses to put the country—and its security—first.”

“Holding a focused and comprehensive hearing on election security is not a partisan or complicated request. It speaks volumes that while Chairman McCaul has been dragging his feet on this issue for over a year, the Senate is holding election security hearings today with current and former homeland security officials. This is all we are asking for. I call on Chairman McCaul to realize his error and follow through on his promise.”

“If Chairman McCaul believes Russia will interfere in the 2018 elections, as he has stated, we cannot ignore this threat. Having hearings on election security—while developing solutions and showing the public that we are working together on this issue is a solid first step. The 2018 elections are only 7 months away and we must be doing much more to protect them. If we do nothing, we are just inviting Putin to what he pleases with our democracy and our domestic affairs.”

PRESS RELEASE—THOMPSON TO SPEAKER RYAN: ELECTION SECURITY BRIEFING
INSUFFICIENT

MAY 15, 2018

(WASHINGTON).—Today, Rep. Bennie G. Thompson (D-MS), Ranking Member of the Committee on Homeland Security, and Co-Chair of the Congressional Task Force on Election Security, released the following statement on news that Speaker Ryan has announced an election security briefing for Members of Congress:

“Unfortunately, due to it being in an unclassified setting, it is not possible for this last-minute briefing scheduled by House Republicans on election security to be able to go into the detail necessary to properly educate Members of Congress on the Trump administration’s efforts—or lack thereof—to secure our election systems from foreign interference. House Republicans have treated election security as a third-rung issue for over a year, it is time for them to finally take this National security issue seriously. The next Federal election is less than 6 months away.”

PRESS RELEASE—THOMPSON: SHOCKING SECRETARY NIELSEN HASN'T READ 2017
INTEL ASSESSMENT, ISN'T AWARE RUSSIA HELPED TRUMP

MAY 22, 2018

(WASHINGTON).—Today, Rep. Bennie G. Thompson (D-MS), Ranking Member of the Committee on Homeland Security, released the following statement on Homeland Security Nielsen's alarming comments after the House of Representative's election security briefing today:

"I was shocked to hear that Secretary Nielsen has apparently not bothered to read the January 2017 intelligence community assessment that Russia interfered in our elections and undermined our democratic process to help President Trump win. This report is over a year old, has stood the test of time, was agreed to by the entire intelligence community, and was backed up by Senate investigators. The fact that she did not seem aware of the report's findings while briefing Members of Congress on the very important topic of election security is appalling to all who have tried to make progress on this issue since 2016 with little help from Republicans or this administration. I sincerely hope the Secretary's comments today were not just rhetorical gymnastics to placate the President.

"Even though this report is widely available, I will be sure to deliver the Secretary a copy. After today's briefing, it is clear that our Government must do more, and whatever possible, to secure our elections from foreign interference. The integrity of our democracy is at stake and comments like those from the Secretary today are not helpful."

PRESS RELEASE—THOMPSON STATEMENT ON MUELLER INDICATING ELECTION
MEDDLING ON-GOING

JUNE 21, 2018

(WASHINGTON).—Today, Rep. Bennie G. Thompson (D-MS), Ranking Member of the Committee on Homeland Security and co-Chair of the Congressional Task Force on Election Security, released the following statement on news from Special Counsel Robert Mueller that election meddling operations are still on-going:

"As Robert Mueller confirmed today, the threat to our elections from foreign interference persists and it is high time the White House wakes up and takes this threat seriously. Inaction will have grave consequences for public confidence in the integrity of our democracy. It is unacceptable that the Government official most directly communicating on the on-going threat to our elections is the Special Counsel.

"President Trump must start acting like the President of the country instead of obsessing over photo ops with Kim Jong-un, saving ZTE jobs in China, and casting aside close allies like Canada to curry favor with Vladimir Putin. Anything less is an abdication of his oath of office. With the mid-term elections less than 5 months away, he must make it clear that election security is the top National security priority and push Republicans in Congress to do more."

It has been over 3 months since Congressman Thompson introduced H.R. 5011, the Election Security Act to help secure our voting systems. The legislation, with 105 co-sponsors, has still not received a hearing or a vote.

TRANSCRIPT

OCTOBER 24, 2017

The transcript for *Securing America's Elections: Preparing for 2018 and Beyond*, Congressional Task Force on Election Security, Committee on House Administration, is retained in the committee files.

CONGRESSIONAL TASK FORCE ON ELECTION SECURITY PRELIMINARY FINDINGS AND
RECOMMENDATIONS

One year ago, 139 million Americans cast their vote in the wake of a massive Russian cyber-enabled influence operation designed to "undermine public faith in the U.S. democratic process, denigrate Secretary [Hillary] Clinton, and harm her electability and potential presidency." Using a vast network of social media trolls, fake "bot" accounts, and state-owned news outlets, the Kremlin spread

disinformation to the American electorate through more than 1,000 YouTube videos, 130,000 tweets, and 80,000 Facebook posts viewed by as many as 150 million people on Facebook platforms alone. They hacked into U.S. political organizations, selectively exposing sensitive personal information about DNC staffers using third-party intermediaries like WikiLeaks. Finally, according to U.S. intelligence reports, Russia targeted voter registration databases in at least 21 States and sought to infiltrate the networks of voting equipment vendors, political parties, and at least one local election board.

Although this election cycle was unlike any before, the U.S. intelligence community warns that it may be the “New Normal.” Recent reports show that the vast majority of U.S. States are still relying on outdated, insecure voting equipment and other election technologies that lack even basic cybersecurity standards. Meanwhile, Republicans in Congress have shown little interest in fighting Russian interference, and have instead chosen to act on measures that would eliminate rather than bolster funding for the Election Assistance Commission (EAC), the Federal agency responsible for helping States secure these vulnerable systems.

With just over a year until the 2018 midterm elections, it is important that we reflect on lessons learned in the last year and focus the spotlight on election security to push for reforms that protect the integrity of the ballot box.

The Congressional Task Force on Election Security has spent the past 5 months working together to understand the threats to election infrastructure and how to address them. The Task Force found:

- *Election security is National security, and our election infrastructure is critical infrastructure.*—Federal law defines critical infrastructure as systems and assets for which “incapacity or destruction . . . would have a debilitating impact on security, National economic security, National public health or safety,” or any combination thereof. Such infrastructure is given priority access to threat intelligence, incident response, technical assistance, and other products and services to help owners and operators harden their defenses. It is hard to imagine a system failure that would inflict more damage than a foreign adversary infiltrating our voting systems to hijack our democratic process. Nonetheless, Trump’s Homeland Security Department (DHS) has wavered on its commitment to honor the Obama administration’s decision to designate election systems as a critical infrastructure subsector. Whether the next Secretary of Homeland Security will take a firm stand and maintain the designation remains to be seen.
- *Our election infrastructure is vulnerable.*—Many elections across our country are being run on equipment that is either obsolete or near the end of its useful life. In over 40 States, elections are carried out using voting machines and voter registration databases created more than a decade ago. These technologies are more likely to suffer from known vulnerabilities that cannot be patched easily, if at all. As we saw at this year’s DEFCON Voting Village, even hackers with limited prior knowledge, tools, and resources are able to breach voting machines in a matter of minutes.
- *These vulnerable systems are being targeted by one of the world’s most sophisticated cyber actors.*—According to the U.S. intelligence community, Russian interference in the 2016 election “demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations,” and warned that “Moscow will apply lessons learned from . . . the U.S. Presidential election to future influence efforts world-wide, including against U.S. allies and their election processes.” We cannot reasonably assume that State voting systems are secure enough to withstand a state-sponsored cyber attack, and we have no reason to believe these attacks will subside.
- *Fortunately, many of the security solutions and best practices are already known.*—We can mitigate many vulnerabilities with existing, time-tested cybersecurity fixes found in the NIST Cybersecurity Framework and the CIS “Top 20” Critical Security Controls. By adopting even the Top 5 security controls, organizations can thwart 85 percent of common cyber attacks. Security experts also tend to agree on the types of voting systems most susceptible to compromise, and are urging election officials to phase out paperless Direct Recording Electronic (DRE) machines, replace these machines with voter-marked paper ballots, and carry out risk-limiting audits to verify election results.
- *Federal agencies like DHS and EAC are important partners in this effort, but they need resources and consistent support from Congress.*—We have a rare window of opportunity to promote the widespread adoption of common-sense security measures that protect the integrity of the ballot box. This is not the time to diminish Federal efforts or shut down important lines of dialog between DHS and election administrators.

DHS is able to provide participating State and local governments with cyber threat intelligence, vulnerability assessments, penetration testing, scanning of databases and operating systems, and other cybersecurity services at no cost. Despite some initial confusion about the critical infrastructure designation, DHS has worked to build relationships with election officials, clarify the voluntary nature of DHS services, resolve disparities in information sharing and victim notification, and assist the subsector in formally establishing a Coordinating Council, which had its first meeting this fall. Where DHS has rendered assistance, officials report that cyber hygiene scans and other services are valuable. However, there is currently a 9-month wait list for Risk and Vulnerability Assessments, and questions remain about how to ensure threat information reaches election officials, many of whom lack security clearances.

The EAC has been a valuable partner to State and county election officials. The agency has played a crucial role in election security by serving as a clearinghouse of information for State and local election officials, facilitating communications between these officials and DHS, providing easy-to-use cybersecurity guidance, and testing and certifying voting machines. Numerous State and local officials have expressed support and appreciation for the agency's work. Unfortunately, in recent years Republicans have made several attempts to terminate the agency. Instead, Congress should support the EAC and provide it with the resources it needs to help States secure their election systems. In addition, the President should nominate and the Senate should confirm a fourth commissioner to the EAC so that the agency can operate with its full slate of commissioners.

In light of its preliminary findings, the Task Force makes the following recommendations:

- *Maintain the designation of election infrastructure as a critical infrastructure subsector.*—This designation ensures that State and local election officials receive prioritized access to DHS's cybersecurity services. Defining election systems as critical infrastructure means these systems will, on a more formal and enduring basis, be a priority for DHS cybersecurity assistance. These services are an important force multiplier, especially at the State and local level, where resources are scarce.
- *Help States fund and maintain secure election systems.*—We cannot ask our State and local election officials to take on a State actor like Russia alone. Although States and counties are largely responsible for elections, Congress has a role to play in helping States fund the purchase of newer, more secure election systems, and requiring such systems adhere to baseline cybersecurity standards. Election officials need money to replace aging voting systems, many of which do not provide an auditable paper trail. It is important to note, however, that cyber threats evolve at a rapid pace, and a one-time lump sum investment is not enough. States also need resources for maintenance and periodic upgrades, and cybersecurity training for poll workers and other election officials.
- *States should conduct post-election risk-limiting audits.*—A risk-limiting audit involves hand counting a certain number of ballots to determine whether the reported election outcome was correct. Risk-limiting audits used advanced statistical methods to enable States to determine that the original vote count was accurate with a high degree of confidence. These audits are useful in detecting any incorrect election outcomes, whether they are caused by a cyber attack or something more mundane like a programming error. Moreover, conducting these audits as a matter of course increases public confidence in the election system.
- *Empower Federal agencies to be effective partners in pushing out Nation-wide security reforms.*—With mid-term elections in a year, election officials cannot afford to wait 9 months for valuable cybersecurity services like Risk and Vulnerability Assessments. At the same time, we cannot ask DHS to deliver election assistance at the expense of its other critical infrastructure customers. We should give DHS the resources it needs to provide election officials with timely assessments and other cybersecurity services, without detracting from its overall critical infrastructure mission. Similarly, Congress should fund EAC at a level commensurate with its expanded role in election cybersecurity and confirm a fourth commissioner so the agency is able to continue to serve as a resource on election administration.
- *Establish clear and effective channels for sharing threat and intelligence information with election officials.*—Effective information sharing is critical to address the decentralized threat that our Nation faces in terms of securing our elections. Prior to the 2016 elections, we have seen how information sharing failures can cause catastrophic events. The 9/11 terrorist attacks exposed seri-

ous gaps in information sharing within the Federal Government and State and local law enforcement partners. It is imperative that election officials have access to the most timely and high-level security information. Chief election officials in each State should have expedited access to security clearances. DHS needs a formalized process to provide real-time appropriate threat information to State and local election officials to improve information flow and help prevent intrusions in our election infrastructure.

- *Prioritize cybersecurity training at the State and local level.*—The events of 2016 demonstrate that human error is a significant vulnerability as it leaves systems open to spear-phishing and other forms of cyber attack. States and localities face the daunting task of training hundreds, if not thousands, of election officials, IT staff, and poll workers on cybersecurity and risk mitigation. It costs money for States to produce training materials, and takes staff time to implement State-wide training programs. The Federal Government should provide training support either through the EAC or by providing funding to States to assist with their training programs.

CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, FINAL REPORT

JANUARY 2018

The document is retained in committee files and is available at: <https://democrats-homeland.house.gov/sites/democrats.homeland.house.gov/files/documents/TFESReport.pdf>.

H.R. 5011

The document is retained in committee files and is available at: <https://www.gpo.gov/fdsys/pkg/BILLS-115hr5011h/pdf/BILLS-115hr5011h.pdf>.

H. RES. 235

The document is retained in the committee files and is available at: <https://www.congress.gov/bill/115th-congress/house-resolution/235/r=1>.

Mr. THOMPSON. H.R. 5011, the Election Security Act, currently has over 100 cosponsors, all Democrats. The legislation would, among other things, provide on-going support to State and local governments to secure election infrastructure, instead of addressing election challenges crisis to crisis; direct the Department of Homeland Security to address the resources it needs to carry out its election security responsibilities, and submit a request to Congress, and establish mechanisms to ensure that State election officials have timely access to actionable threat information.

I have asked the committee to consider H.R. 5011 and today renew my request for consideration of this legislation. Even though Congress appropriated some additional funding for DHS and the States to improve election security in the fiscal year 2018 omnibus, it was merely a downpayment of what is required. H.R. 5011 would help provide the States with the appropriate level of funding.

Today's other witness, Rhode Island's secretary of state, Nellie Gorbea, participated in one of our task force forums in October. She provided important insight into the resources the Federal Government was making available to States, the resources States need to secure election infrastructure, and proactive activities she was undertaking at the State level to improve election security.

I am glad that the secretary is here with us today. Again, I look forward to her and Under Secretary Kreb's testimony. Securing our elections is part and parcel to securing our Democracy.

With that, Mr. Chair, I yield back.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JULY 11, 2018

Under Secretary Krebs, you have taken this job at a critical moment for our Nation; however, I am concerned you do not have the support you need from the White House. You are responsible for building private-sector confidence in DHS's information-sharing programs like Automated Indicator Sharing, after President Trump toyed with the idea of planting an absurd story to discredit it for his own political purposes.

You are responsible for securing Federal networks at a time when the White House's National Security Advisor has decided to eliminate the National Security Council's cybersecurity coordinator. You are responsible for helping secure critical infrastructure networks for a White House that would rather save jobs in China than heed the advice of the intelligence community on supply chain vulnerabilities. And you are responsible for helping State and local governments secure election infrastructure following Russia's brazen election meddling efforts in 2016, which the President has been reluctant to call out and which Congressional Republicans, until recently, were content to ignore.

As we sit here today, President Trump is in Europe complicating your mission. Instead of working with our European allies to confront Russia—a shared adversary whose attempts to undermine Western democratic institutions are growing more and more bold—he is trolling them to curry favor with Russian President Vladimir Putin. President Trump has said he will address Russia's 2016 election meddling in a meeting with Putin, but he has never demonstrated a credible ability to confront Putin with our intelligence community's findings. He has predicted his meeting with Putin “may be the easiest,” so I have no reason to believe anything productive will come of it. This President's failure to take seriously the threat to our democracy is one of the main reasons that we must do effective and thorough oversight in this body.

Although I am pleased that the Majority has finally scheduled today's hearing, I am disappointed that the Majority failed to invite a full range of stakeholders, including the Election Assistance Commission, or hold the hearing at a time when DHS's Federal partners were available to participate. It is important to note for the record that committee Democrats have been requesting official oversight activities on election security since before the 2016 election.

And in March 2017, after months of inaction by the Republican majority, I introduced a Resolution of Inquiry seeking information from the Department on its activities related to countering Russian election interference in the 2016 Presidential election so we would understand how to protect our elections in the future. It was unceremoniously rejected along party lines.

Committee Democrats have written to the Chairman no less than five times since August 2016 to request a hearing, briefing, or investigation on vulnerabilities to our election infrastructure. We have also reiterated these requests on numerous occasions on the record. Despite these repeated requests, this committee did not conduct a formal hearing or briefing on the topic until April 2018—15 months after the intelligence community released its report concluding that the Russian government had attempted to interfere in the 2016 elections and would attempt to do so again.

When the Trump administration's six top intelligence officials testified before the Senate that Russia was targeting our 2018 elections, this committee—the committee that prides itself on acting in the wake of current issues—followed suit of the House Republican Conference by shirking its responsibility to act on this urgent threat.

Ranking Members of the Oversight and Government Reform Committee, the Foreign Affairs Committee, Judiciary Committee, the Permanent Select Committee on Intelligence, the House Armed Services, and the House Administration Committee have all urged their Chairs or Speaker Ryan to aggressively address this on-going National security threat. Our calls for action were ignored, responded to with a half-hearted acknowledgement of the threat and a vague promise for future action, or the offer to ask a Government witness about election security at a hearing on another topic.

Because our requests for thorough hearings and briefings were denied, some committee Democrats joined with Democrats on the Committee on House Administration to form the Congressional Task Force on Election Security. I openly asked Republicans to join us and submit their ideas, yet no Republican Member provided their input or attended the task force's public events.

After studying the topic for 8 months, meeting with stakeholders, and holding a series of forums and briefings, the Task Force produced a report and introduced legislation to implement the recommendations. H.R. 5011, the Election Security Act, currently has over 100 co-sponsors—all Democrats. The legislation would, among other things:

- provide on-going support to State and local governments to secure election infrastructure, instead of addressing election challenges crisis-to-crisis;
- direct the Department of Homeland Security to assess the resources it needs to carry out its election security responsibilities and submit a request to Congress; and
- establish mechanisms to ensure that State election officials have timely access to actionable threat information.

I have asked this committee to consider H.R. 5011, and today renew my request for consideration of this legislation. Even though Congress appropriated some additional funding for DHS and the States to improve election security in the fiscal year 2018 omnibus, it was merely a down-payment on what is required. H.R. 5011 would help provide the States with the appropriate level of funding.

Today's other witness, Rhode Island Secretary of State Nellie Gorbea, participated in one of our Task Force forums in October. She provided important insight into the resources the Federal Government was making available to States, the resources States need to secure election infrastructure, and proactive activities she was undertaking at the State level to improve election security. I am glad that Secretary Gorbea is here with us again today, and I look forward to her and Under Secretary Krebs' testimony. Securing our elections is part and parcel to securing our democracy.

Chairman MCCAUL. The Ranking Member yields back.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Hon. Jackson Lee follows:]

STATEMENT OF HON. SHEILA JACKSON LEE

JULY 11, 2018

Chairman McCaul and Ranking Member Thompson thank you for holding today's hearing so that the committee may learn more about "DHS Progress in Security Election Systems and Other Critical Infrastructure."

I thank today's witnesses:

- The Honorable Christopher Krebs, Under Secretary, National Protection and Programs Directorate with the Department of Homeland Security; and
- The Honorable Nellie Gorbea, Secretary of State, State of Rhode Island.

I thank each of you for bringing your expert view of the cyber threats against our Nation's system of elections and other matters regarding the security of critical infrastructure.

The House Committee on Homeland Security has the responsibility of providing for the cybersecurity of Federal civilian agencies as well as the to secure the Nation's 16 critical infrastructure sectors from cyber and other threats.

On January 6, 2017, Homeland Security Secretary Johnson designated election systems as critical infrastructure, and created a new subsector under the existing Government Facilities Sector designation.

The Election Infrastructure Subsector covers a wide range of physical and electronic assets such as storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of State and local governments.

The process established for contacting and working with local and State elections administrators seems to be working well.

The work to secure our Nation's election system from cyber threats is on-going, which is why this hearing is relevant.

The U.S. Department of Homeland Security's (DHS) mission in cybersecurity and infrastructure protection is focused on enhancing greater collaboration on cybersecurity across the 16 critical infrastructure sectors and the sharing of cyber threat information between the private sector and Federal, State, and local partners.

I thank Ranking Member Thompson for his leadership in co-chairing the Congressional Task Force on Election Security, which issued a report earlier this year which outlined areas of concern regarding the security of election systems.

Leader Pelosi convened the Task Force after waiting a year for the leadership of the House to investigate Russian interference in the 2016 U.S. Elections.

We know the threats that computing devices and systems face, which are almost too numerous to count:

- Bot-nets;
- Ransom-ware;
- Zero Day Events;
- Mal-ware;
- Denial of Service Attacks;
- Distributed Denial-of-Service Attacks;
- Pharming;
- Phishing;
- Data Theft;
- Data Breaches;
- SQL Injection;
- Man-in-the-middle attack.

The list goes on, but suffice it to say that as hard as one person in our Government is working to stop cyber attacks there are likely another thousand attempting to breach a system or device owned by a United States citizen.

This is why I introduced H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act, which passed the House earlier this year.

The bill requires the Secretary of Homeland Security to submit a report on the policies and procedures developed for coordinating cyber vulnerability disclosures.

The report will include an annex with information on instances in which cybersecurity vulnerability disclosure policies and procedures were used to disclose details on identified weaknesses in computing systems that or digital devices at risk.

The report will provide information on the degree to which the information provided by DHS was used by industry and other stakeholders.

The report may also contain a description of how the Secretary of Homeland Security is working with other Federal entities and critical infrastructure owners and operators to prevent, detect, and mitigate cyber vulnerabilities.

The reason that I worked to bring this bill before the full House for consideration is the problem often referred to as a “Zero Day Event.”

A Zero Day Event describes the situation that network security professionals may find themselves when a previously unknown error or flaw in computing code is exploited by a cybercriminal or terrorist.

The term “Zero Day Event” simply means that there is zero time to prepare a defense against a cyber attack.

When a defect in software is discovered then network engineers and software companies can work to develop a “patch” to fix the problem before it can be exploited by those who may seek to do harm.

H.R. 3202 seeks a report on the on-going Department of Homeland Security’s policies and procedures for coordinating cyber vulnerability disclosures such as Zero Day Events with private-sector partners.

Because vulnerabilities can be used by adversaries it is important that this sensitive information be managed securely so details are not routinely made available neither to the public nor to Congress.

H.R. 3202 provides the Congress with the opportunity to understand the process and procedures used by the Department of Homeland Security and the benefit these disclosures may have for private-sector entities participating in programs in support of cybersecurity.

During the 2016 election we learned of new threats from cyber space that go far beyond any that would have been considered in previous elections.

Russia targeted our Presidential Election according to the report, “Background to Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution,” provided by the Office of the Director of National Intelligence’s National Intelligence Council.

Russia used every cyber espionage tool available to influence the outcome of the Presidential election by using a multi-faceted campaign that included theft of data; strategically timed release of stolen information; production of fake news; and manipulation of facts to avoid blame.

The Russian General Staff Main Intelligence Directorate (GRU) is suspected by our intelligence agencies of having begun cyber operations targeting the United States election as early as March 2016.

They took on the persona of “Guccifer 2.0,” “DCLeaks.com,” and Wikileaks as the identities that would be reported as having involvement in the work they had undertaken to undermine our Nation’s Presidential election.

Russia is blamed for breaching 21 local and State election systems, which they studied extensively.

In February 2018, special counsel Robert Mueller released indictments of 13 Russians, at least one of whom has direct ties to Russian President Vladimir Putin.

The 37-page indictment details the actions taken to interfere with the U.S. political system, including the 2016 U.S. Presidential election.

Among the charges, which include charges for obstruction of justice, are several especially notable details.

The indictment states that 13 defendants posed as U.S. persons and created false U.S. personas and operated social media pages and groups designed to attract U.S. audiences.

The social media profiles “addressed divisive U.S. political and social issues” and falsely claimed to be controlled by U.S. activists.

The defendants are also accused of using “the stolen identities of real U.S. persons to post on social media accounts” which, over time, became the chosen “means to reach significant numbers of Americans for purposes of interfering with the U.S. political system, including the Presidential election of 2016.”

The goal of the effort was to sow discord in the U.S. political system, including the 2016 U.S. Presidential election.

The internet does not sleep—and nor do our Nation’s on-line adversaries.

That Russia used cyber intrusions to attack United States political institutions to collect data to manipulate the media and the public with the purpose of influencing the outcome of the 2016 Presidential elections is now an undisputed fact.

The United States has enemies in other corners of the globe who would not hesitate to attack our election system if given the chance.

These foreign adversaries do not share our commitment to democracy, liberty, and human rights, or the precious freedoms we hold dear.

This Congress must do its job and delve into the issue of Russian involvement in our National election.

The work today must focus on election recovery should a serious cyber incident occur during an election.

Vulnerabilities of computing systems are not limited to intentional attacks, but can include acts of nature, human error, or technology failing to perform as intended.

I am particularly concerned that so many jurisdictions rely on electronic poll books, to check in voters before issuing them ballots, with no paper backups; and the use of paperless electronic voting machines without sufficient paper ballot options in polling locations should they be needed.

The right and better approach to election cybersecurity is to be prepared and not need options for voters to cast ballots, should voting systems fail, rather than being unprepared and needing options for voters to cast ballots during an election.

We must be steadfast in our resolve to have a strong shield to defend civilian and critical infrastructure networks for all threats foreign and domestic.

I look forward to the testimony of today’s witnesses.

Thank you.

Chairman MCCAUL. Just for the record, we had the Secretary testify before this committee, it was openly available on this topic. We had a Classified briefing for all House members on election security.

We have been waiting for Under Secretary Krebs to get confirmed by the Senate, and, sir, we just congratulate on your confirmation by the U.S. Senate. We are fortunate, now, to have you here today to talk about this issue. I also think that the administration is going to be well-served by you, sir, and they are lucky to have you.

On June 15, 2018, Chris Krebs was sworn in as the under secretary for the Department of Homeland Security’s National Protection and Programs Directorate after being confirmed by the Senate by a voice vote. As under secretary, Mr. Krebs oversees NPPD’s efforts to defend civilian networks, secure Federal facilities, manage systemic risk to National critical functions, and work with stakeholders to raise the security baseline of the Nation’s cyber and physical infrastructure.

This is his second tour working at DHS, previously serving as a senior advisor to the assistant secretary for infrastructure protection and playing a formative role in a number of National and international risk management programs. I appreciate your leadership in both the private and the public sectors, sir. Thank you for being here.

I now would like to yield to Mr. Langevin from Rhode Island to introduce the Rhode Island secretary of state.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank you and Ranking Member Thompson for reaching out to me to facilitate inviting Rhode Island Secretary of State Nellie Gorbea here to the committee for—to hear her testimony and the progress she has made in securing election—Rhode Island’s election systems.

Before I introduce Secretary Gorbea, I just want to take a moment to publicly congratulate Secretary Krebs on his finally being confirmed, officially. We had a brief conversation and wanted to publicly, again, congratulate you, Secretary. I appreciate the on-going relationship and work that you and I have done together, and discussions we have had on election and cybersecurity, in particular election security. I hope that dialog can continue in our working together.

But Mr. Chairman and Ranking Member Thompson, very proud, today, to be honored—to be able to recognize and welcome Nellie Gorbea, Rhode Island’s secretary of state, to the panel, today.

Secretary Gorbea has helped position the Ocean State as a leader in election security. Under her direction, Rhode Island replaced all of its two-decades-old voting equipment prior to the 2016 election with new paper ballot systems. Following the 2016 elections, Secretary Gorbea has taken all the steps that we need—that we would hope for States to take to better secure their elections systems.

She has emphasized proper I.T. staffing and training, solicited help from the Election Assistance Commission and from DHS and proactively exchanged information with peers through the Multi-State ISAC, Elections Infrastructure ISAC, and the National Association of Secretaries of State.

Now, with the help of Federal grants appropriated by this Congress, Secretary Gorbea is directing the overhaul of Rhode Island’s voter registration database, initiating local level grants to increase security and implementing the country’s second mandatory post-election risk limiting audit process. Just as importantly, Secretary Gorbea has implemented reforms to increase voter access to the polls in Rhode Island, including on-line and automated voter registration.

Secretary Gorbea, thank you for making the trip down from Rhode Island to here, today, with us. Thank you for your on-going efforts to expand Rhode Island’s access to the polls, and to prevent foreign adversaries’ access to the same.

Mr. Chairman, this is a position that I once held as Rhode Island secretary of state. I am very proud and grateful for the leadership that Secretary Gorbea has continued to provide and has, certainly, exceeded even things that I have accomplished when I was there, and I am very proud of what she has done. I hope you and all of our colleagues take the opportunity to ask the secretary about her

successes and how Rhode Island's leadership can be a model for other States to follow.

Thank you, Mr. Chairman. With that, I yield back.

Chairman MCCAUL. The gentleman yields back. Thank you, both, for being here today. Your full written statements will appear in the record.

The Chair now recognizes Under Secretary Krebs for an opening statement.

**STATEMENT OF CHRISTOPHER C. KREBS, UNDER SECRETARY,
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE,
U.S. DEPARTMENT OF HOMELAND SECURITY**

Under Secretary KREBS. Chairman McCaul, Ranking Member Thompson, and Members of the committee, thank you for today's opportunity to testify regarding the Department of Homeland Security's on-going efforts to assist State and local election officials, those who own and operate election systems, with improving the resilience of election security across America.

Today's hearing is timely as primary elections are, generally, complete. Election officials now have some time to reflect and get ready for the November mid-term elections. In fact, later this week, our leadership team at DHS will meet with election officials as they gather in Philadelphia for their National summer conference.

It is not lost on me that we will discuss defending our democratic institutions and the very cradle of democracy, the city that birthed this great Nation. The 2018 mid-terms remain a potential target for Russian actors, but the intelligence community has yet to see any evidence of a robust campaign aimed at tampering with our election infrastructure along the lines of 2016 or influencing the makeup of the House or Senate races.

The intelligence community, however, continues to see Russia using social media flag—false flag personas, sympathetic spokesmen, and other means to influence or inflame positions on opposite ends of controversial issues. These efforts appear to be more focused on dividing rather than targeting specific politicians or political candidates. Nonetheless, we remain vigilant and any attempt to undermine our democracy will be met with consequences. In the mean time, we will continue to work with our election partners to strengthen the resilience of our election systems.

As I have traveled across the country during primary season, it is clear to me that secretaries of state and other election officials are not sitting back; they take cybersecurity and security in general seriously. Our mission at DHS is to help our stakeholders better understand and manage the risks they face.

Through concerted efforts, in part by building relationships, establishing trust, and understanding what it is that our stakeholders need to manage their risks, we have made significant progress over the last year-and-a-half. Working with State and local election officials, as well as with private-sector partners who support them, we have created Government and private-sector councils who, collaboratively, work to share information, promote best practices, and develop strategies to reduce risk to the Nation's election systems.

We have also created the Election Infrastructure Information Sharing and Analysis Center, or ISAC, made up of over 1,000 members in just under 5 months, including all 50 States. We are also sponsoring security clearances for multiple election officials in each State. We have increased the availability and deployment of free technical services.

We have also offered cybersecurity and physical security training and exercises and later this summer, we will have a 3-day tabletop exercise with all States involved. Our suite of services will continue to mature as the requirements identified by our election stakeholders mature.

We understand that the only way to deliver a resilient election system is to work, collaboratively, with those election—with those officials on the front lines running the process. Our work to secure election officials—I am sorry—to secure election infrastructure is part of my directorate's broader mission to secure all of our Nation's critical infrastructure.

We are responsible for coordinating the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. As we confront—confront threats posed by a range of capable adversaries, DHS remains focused on ensuring National unity of effort. It is critical that we combine the unique expertise of the intelligence community, law enforcement, sector-specific agencies, and others, to provide an integrated approach to risk management across our Nation's critical infrastructure.

Rarely is a cyber event sector-specific. Our adversaries target systems that are cross-sector and the growing interdependencies across sectors demand this integrated approach. Accordingly, DHS serves as information and operations integrator focused on delivering cross-sector public-private risk management strategies to enhance the resilience of our Nation's infrastructure.

Before I conclude, I would like to take a moment to thank Congress and this committee in particular for legislative progress thus far in strengthening DHS's cybersecurity and critical infrastructure authorities. Specifically, we strongly support final passage of legislation to create the Cybersecurity and Infrastructure Security Agency, SISA, at DHS which would rename and reorganize the National Protection and Programs Directorate. This change reflects the important work we carry out every day to safeguard and secure our critical infrastructure.

Thank you and I look forward to your questions.

[The prepared statement of Secretary Krebs follows:]

PREPARED STATEMENT OF CHRISTOPHER C. KREBS

JULY 11, 2018

Chairman McCaul, Ranking Member Thompson, and Members of the committee, thank you for today's opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) on-going efforts to assist with reducing and mitigating risks to our election infrastructure. DHS is eager to share with you the progress we have made to establish trust-based partnerships with our Nation's election officials who administer our democratic election processes.

Safeguarding and securing cyber space is a core homeland security mission. DHS is responsible for protecting civilian Federal Government networks and collaborating with other Federal agencies, as well as State, local, Tribal, and territorial governments, and the private sector to defend against cyber threats. We endeavor to enhance cyber threat information sharing across the globe to stop cyber incidents be-

fore they start and help businesses and Government agencies to protect their cyber systems and quickly recover should such an attack occur. By bringing together all levels of government, the private sector, international partners, and the public, we are taking action to protect against cybersecurity risks, improve our whole-of-Government incident response capabilities, enhance information sharing of best practices and cyber threats, and to strengthen resilience.

Recognizing that the 2018 U.S. mid-term elections are a potential target for malicious cyber activity, DHS is committed to robust engagement with State and local election officials, as well as private-sector entities, to assist them with defining their risk, and providing them with information and capabilities that enable them to better defend their infrastructure.

Given the foundational role that elections play in a free and democratic society, in January 2017 the Secretary of Homeland Security designated election infrastructure as a critical infrastructure subsector. Under our system of laws, Federal elections are administered by State and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security and resilience on a day-to-day basis.

As such, DHS and our Federal partners have formalized the prioritization of voluntary cybersecurity assistance for election infrastructure similar to that which is provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities.

Since 2016, DHS's National Protection and Programs Directorate (NPPD) has convened Federal Government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. The Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives, including plans for EIS engagement and the establishment of a sector-specific plan (SSP). GCC representatives include DHS, the Election Assistance Commission (EAC), and 24 State and local election officials. Participation in the council is entirely voluntary and does not change the fundamental role of State and local jurisdictions in overseeing elections.

The Department and the EAC worked with election industry representatives to launch an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with leadership designated by the sector membership. The SCC serves as industry's principal entity for coordinating with the Government on critical infrastructure security activities and issues related to sector-specific strategies and policies. This collaboration is conducted under DHS's authority to provide a forum in which Government and private-sector entities can jointly engage in a broad spectrum of activities to coordinate critical infrastructure security and resilience efforts which is used in each of the critical infrastructure sectors established under Presidential Policy Directive 21, Critical Infrastructure Security and Resilience. The process is a well-tested mechanism across critical infrastructure sectors for sharing threat information among the Federal Government and critical infrastructure partners, advancing risk management efforts, and prioritizing services available to sector partners in a trusted environment.

NPPD also engages directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident coordination, resources, and services. In order to ensure a coordinated approach from the Federal Government, NPPD has convened stakeholders from across the Federal Government through an Election Task Force. The task force serves to provide actionable information and offer assistance to assist election officials with strengthening their election infrastructure by reducing and mitigating cyber risk, and increasing resilience of their processes.

Within the context of today's hearing, I will address the unclassified assessment of malicious cyber operations directed against U.S. election infrastructure and our efforts to help enhance the security of elections that are administered by jurisdictions around the country.

ENHANCING SECURITY FOR FUTURE ELECTIONS

DHS regularly coordinates with the intelligence community and law enforcement partners on potential threats to the homeland. Among non-Federal partners, DHS has been engaging State and local officials, as well as relevant private-sector entities, to assess the scale and scope of malicious cyber activity potentially targeting the U.S. election infrastructure. Election infrastructure includes the information and communications technology, capabilities, physical assets, and technologies that enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.

DHS is committed to ensuring a coordinated response from DHS and its Federal partners to plan for, prepare for, and mitigate risk to election infrastructure. We understand that working with election infrastructure stakeholders is essential to ensuring a more secure election. DHS and our stakeholders are increasing awareness of potential vulnerabilities and providing capabilities to enhance the security of U.S. election infrastructure as well as that of our democratic allies.

Election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and on-going engagements, DHS is working to provide value-added—yet voluntary—services to support their efforts to secure elections.

Improving Coordination with State, local, Tribal, Territorial (SLTT) and private-sector partners.—Increasingly, the Nation’s election infrastructure leverages information technology (IT) for efficiency and convenience, but also exposes systems to cybersecurity risks, just like in any other enterprise environment. Just like with other sectors, NPPD helps stakeholders in Federal departments and agencies, SLTT governments, and the private sector to manage these cybersecurity risks. Consistent with our long-standing partnerships with State and local governments, we have been working with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

The National Cybersecurity and Communications Integration Center (NCCIC) works with the MS-ISAC to provide threat and vulnerability information to State and local officials. For nearly a decade, DHS has funded the Multi-State Information Sharing and Analysis Center (MS-ISAC), which has since created the EI-ISAC, to enable its members to share cybersecurity information and collaborate with each other. The EI-ISAC’s membership includes almost 1,000 SLTT election-specific entities. Through the MS-ISAC, it has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for State chief information officers.

Providing Technical Assistance and Sharing Information. NPPD actively promotes a range of services including:

Cyber hygiene service for internet-facing systems.—Through this automated, remote scan, NPPD may provide a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the internet, such as on-line voter registration systems, election night reporting systems, and other internet-connected election management systems.

Risk and vulnerability assessments.—We have prioritized State and local election systems upon request, and increased the availability of risk and vulnerability assessments (RVAs). These in-depth, on-site evaluations include a system-wide understanding of vulnerabilities, focused on both internal and external systems. We provide a full report of vulnerabilities and recommended mitigations following the testing.

Incident response assistance.—We encourage election officials to report suspected malicious cyber activity to the NCCIC. Upon request, the NCCIC can provide assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the Federal Government’s ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other State officials so they have the ability to defend their own systems from similar malicious activity.

Knowing what to do when a security incident happens—whether physical or cyber—before it happens, is critical. NPPD supports election officials with incident response planning including participating in exercises and reviewing incident response playbooks. Crisis communications are a core component of these efforts, ensuring officials are able to communicate transparently and authoritatively to their constituents when an incident unfolds. In some cases, we do this directly with State and local jurisdictions. In others, we partner with outside organizations. We recognize that securing our Nation’s systems is a shared responsibility, and we are leveraging partnerships to advance that mission.

Information sharing.—NPPD maintains numerous platforms and services to share relevant information on cyber incidents. State election officials may also receive information directly from the NCCIC. The NCCIC also works with the EI-ISAC, which allows election officials to connect with the EI-ISAC or their State chief information officer to rapidly receive information they can use to protect their systems. Best practices, cyber threat information, and technical indicators, some of which had been previously Classified, have been shared with election officials in thousands of State and local jurisdictions. In all cases, the information sharing and/or use of such cybersecurity risk indicators, or information related to cybersecurity risks and inci-

dents complies with applicable lawful restrictions on its collection and use and with DHS policies protective of privacy and civil liberties.

Classified information sharing.—To most effectively share information with all of our partners—not just those with security clearances—we work with the intelligence community to rapidly declassify relevant intelligence or provide tearlines. While DHS prioritizes declassifying information to the extent possible, we also provide Classified information to cleared stakeholders, as appropriate. DHS has been working with State chief election officials and additional election staff in each State to provide them with security clearances. By working with ODNI and the Federal Bureau of Investigation (FBI), in February 2018 election officials from each State received 1-day read-ins for a Classified threat briefing while they were in Washington, DC. This briefing demonstrated our commitment to ensuring election officials have the information they need to understand the threats they face.

Field-based cybersecurity advisors and protective security advisors.—NPPD has more than 130 cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems; and to secure the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources.—NPPD provides guidance and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active-shooter scenarios, and what to do if they suspect an improvised explosive device.

ELECTION SECURITY EFFORTS MOVING FORWARD

DHS has made tremendous strides and is committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. The establishment of Government and sector-coordinating councils will build the foundations for this enduring partnership not only in 2018, but for future elections as well. We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. However, we recognize that there are significant technology needs across SLTT governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that election systems across the Nation are upgraded and secure, with vulnerable systems retired. These efforts require a whole-of-Government approach. The President and this administration are committed to addressing these risks.

There is a fundamental link between public trust in our election infrastructure and the confidence the American public places in basic democratic functions. Ensuring the security of our electoral process is a vital National interest and one of our highest priorities. Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, we will continue to work with Federal agencies, State and local partners, and private-sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

NATIONAL RISK MANAGEMENT

In addition to addressing election security, we coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure, and is responsible for administering the implementation of Federal Government cybersecurity policies and practices. Cyber threats remain one of the most significant strategic risks for the United States, threatening our National security, economic prosperity, and public health and safety. We have long been confronted with myriad attacks against our digital networks. Americans have seen advanced persistent threat actors, including hackers, cyber criminals, and nation-states, increase the frequency and sophistication of these attacks. Our adversaries have been developing and using advanced cyber capabilities to undermine critical infrastructure, target our livelihoods and innovation, steal our National security secrets, and threaten our democracy.

Global cyber incidents, such as the "WannaCry" ransomware incident and the "NotPetya" malware incident in May and June 2017, respectively, are examples of malicious actors leveraging cyber space to create disruptive effects and cause economic loss. These incidents exploited known vulnerabilities in software commonly

used across the globe. Prior to these events, NPPD had already taken actions to help protect networks from similar types of attacks. Through requested vulnerability scanning, we helped stakeholders identify vulnerabilities on their networks so they could be patched before incidents and attacks occur. Recognizing that not all users are able to install patches immediately, we shared additional mitigation guidance to assist network defenders. As the incidents unfolded, we led the Federal Government's incident response efforts, working with our interagency partners, including providing situational awareness, information sharing, malware analysis, and technical assistance to affected entities.

In a series of incidents since at least May of last year, working with U.S. and international partners, DHS and FBI have identified Russian government actors targeting Government entities and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors. DHS assesses that this campaign ultimately collected information pertaining to industrial control systems with the intent to gain access to industrial control systems environments. The intrusions have been comprised of two distinct categories of victims: Staging and intended targets. In other words, through the Department's incident response actions, we have observed this advanced persistent threat actor target certain entities that then become pivot points, leveraging existing relationships between the initial victim and the intended targets to hide their activity, as part of a multi-stage intrusion campaign to gain access to networks of major, high-value assets that operate components of our Nation's critical infrastructure. Based on our analysis and observed indicators of compromise, DHS has confidence that this campaign is still on-going, and threat actors are actively pursuing their ultimate long-term campaign objectives. DHS and the FBI have published a joint technical alert to enable network defenders to identify and take action to reduce exposure to this malicious activity.

CYBERSECURITY PRIORITIES

This administration has prioritized protecting and defending our public and economic safety from the range of threats that exist today, including those emanating from cyber space. Last year, the President signed Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This Executive Order set in motion a series of assessments and deliverables to understand how to improve our defenses and lower our risk to cyber threats. This order also emphasized the importance of accountability—clarifying that Department and agency heads are responsible and will be held accountable for the security of their networks and systems. NPPD plays an important role in providing capabilities, services, and direction to Federal agencies.

Across the Federal Government, agencies have been implementing action plans to use the industry-standard National Institute of Standards and Technology (NIST) Cybersecurity Framework. Agencies are reporting to DHS and the Office of Management and Budget (OMB) on their cybersecurity risk mitigation and acceptance choices. In coordination with OMB, DHS is evaluating the totality of these Agency reports in order to comprehensively assess the adequacy of the Federal Government's overall cybersecurity risk management posture.

Although Federal agencies have primary responsibility for their own cybersecurity, DHS provides a common set of security tools that helps agencies manage their cyber risk. NPPD's assistance to Federal agencies includes: (1) Providing tools to safeguard civilian Executive branch networks through the National Cybersecurity Protection System (NCPS), which includes "EINSTEIN" and Continuous Diagnostics and Mitigation (CDM) programs, (2) measuring and motivating agencies to implement policies, directives, standards, and guidelines, (3) serving as a hub for information sharing and incident reporting, and (4) providing operational and technical assistance, including threat information dissemination and risk and vulnerability assessments, as well as incident response services. The NCCIC is the civilian government's hub for cybersecurity information sharing, asset incident response, and coordination for both critical infrastructure and the Federal Government.

DHS conducts a number of activities to measure agencies' cybersecurity practices and works with agencies to improve risk management practices. The Federal Information Security Modernization Act of 2014 (FISMA) provided the Secretary of Homeland Security with the authority to develop and oversee implementation of Binding Operational Directives (BOD) to agencies. In May 2018, the Secretary issued a BOD to update a previous BOD related to securing High-Value Assets—those assets, Federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to U.S. National security interests, foreign relations, the econ-

omy, or to the public confidence, civil liberties, or public health and safety of the American people.

NPPD works with interagency partners to prioritize High-Value Assets for assessment and remediation activities across the Federal Government. For instance, we conduct security architecture reviews on these High-Value Assets to help agencies assess their network architecture and configurations. The updated BOD enhances NPPD's approach to conducting these engagements to provide agencies with improved results and finding by expanding system scope, refining assessment methodologies, and using less-constrained penetration testing approaches to resemble tactics, techniques, and procedures used by advanced threat actors attempting to gain unauthorized access.

As part of the effort to secure High-Value Assets, DHS conducts in-depth vulnerability assessments of prioritized agency these assets to determine how an adversary could penetrate a system, move around an agency's network to access sensitive data, and exfiltrate such data without being detected. These assessments include services such as penetration testing, wireless security analysis, and "phishing" evaluations in which DHS hackers send emails to agency personnel and test whether recipients click on potentially malicious links. DHS has focused these assessments on Federal systems that may be of particular interest to adversaries or support uniquely significant data or services. These assessments provide system owners with recommendations to address identified vulnerabilities. DHS provides these same assessments, on a voluntary basis upon request, to private-sector and State, local, territorial, and Tribal partners. DHS also works with the General Services Administration to ensure that contractors can provide assessments that align with our HVA initiative to agencies.

In addition to efforts to protect Government networks, Executive Order 13800 requires continued examination of how the Federal Government and industry work together to protect our Nation's critical infrastructure, prioritizing deeper, more collaborative public-private partnerships in threat assessment, detection, protection, and mitigation. In collaboration with civilian, defense, and intelligence agencies, we have worked to identify authorities and capabilities that agencies could employ, soliciting input from the private sector, and developed recommendations to support the cybersecurity efforts of those critical infrastructure entities at greatest risk of attacks that could result in catastrophic impacts.

As part of this effort, DHS is establishing a program office to strengthen support to such entities and improve coordination of interagency support. Through the program office, we will coordinate with Federal and non-Federal partners to enhance access to Classified information, improve incident communication and coordination, and improve cross-sector information sharing, among other efforts.

CONCLUSION

In the face of increasingly sophisticated threats, DHS employees stand on the front lines of the Federal Government's efforts to defend our Nation's critical infrastructure from natural disasters, terrorism and adversarial threats, and technological risk such as those caused by cyber threats. Our infrastructure environment today is complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient. Technological advances have introduced the "Internet of Things" and cloud computing, offering increased access and streamlined efficiencies, while increasing our footprint of access points that could be leveraged by adversaries to gain unauthorized access to networks. As our Nation continues to evolve and new threats emerge, we must integrate cyber and physical risk in order to understand how to effectively secure it. Expertise around cyber-physical risk and cross-sector critical infrastructure interdependencies is where NPPD brings unique expertise and capabilities.

We must ensure that NPPD is appropriately organized to address cybersecurity threats both now and in the future, and we appreciate this committee's leadership in working to establish the Cybersecurity and Infrastructure Security Agency. As the committee considers these issues, we are committed to working with Congress to ensure that this effort is done in a way that cultivates a safer, more secure, and resilient homeland.

Thank you for the opportunity to appear before the committee today, and I look forward to your questions.

Chairman McCAUL. Thank you under secretary and I look forward to working with you to make sure the Senate passes SISA. I think it is important not only to protecting all 16 critical infrastructures but also our election system.

Chair now recognizes the Secretary of State Gorbea for an opening statement. Do you have a microphone?

**STATEMENT OF NELLIE M. GORBEA, SECRETARY OF STATE,
STATE OF RHODE ISLAND**

Ms. GORBEA. Good morning and thank you, Chairman McCaul, Ranking Member Thompson, and Members of the committee for the invitation to participate in this important discussion. I commend your committee for holding this hearing to learn more about what is being done at the Federal, State, and local levels to protect our Nation's election systems and what can be done to improve upon this work.

Advances in technology have brought with them a paradigm shift in elections administration. Cybersecurity is at the forefront of elections conversations taking place right now at every level of government across the country. But before I continue, I want to recognize and thank Congressman Jim Langevin for his visionary leadership in elections administration and his past service as Rhode Island's Secretary of State and whose shoulders I definitely stand on as I do the work I do today.

Today Rhode Island, and almost all other States, face new challenges that can be summarized as follows.

First, although this is not currently the case in Rhode Island, many elections across our country are being run on equipment that is either obsolete or near the end of its useful life; second, our public-sector employees and systems of the State, county, and municipal levels, are ill-prepared to handle the looming threats of cyber attacks.

Finally, our country is facing a very real threat by foreign actors and others looking to erode the public's trust in the integrity of our elections. These attacks are real and are focused on undermining our representative democracy.

On behalf of my colleagues who oversee elections across the country, I do want to thank you for the \$380 million in additional Help America Vote Act funds. However, the challenges our democracy faces today require an on-going commitment of funding so election officials can prepare for threats that were nonexistent 5 years ago.

As these threats involve funding, training and improved communications are critical to protecting our democracy. This funding should be flexible. After all, actions addressing this new landscape of elections and cybersecurity have taken place in a variety of ways because elections are organized and run differently in every State.

Having said that, I do believe that our efforts in Rhode Island over the past 3 years, offer valuable insight into the challenges and opportunities that election officials face in this area of increased cyber threats; so, how has Rhode Island handled these three challenges I described?

First, we replaced outdated voting equipment which was on the brink of failure. We invested nearly \$10 million in new paper-based elections equipment that has four layers of security and encryption. Federal assistance was important throughout all of this process; the election assistance commission helped us for example with the RFVs for that equipment. While modernizing the electoral process and infrastructure, we also leveraged resources offered by the De-

partment of Homeland Security under the Critical Infrastructure Designation.

We further protected our central voter registration system. For example, recently the Department of Homeland Security performed external penetration testing and vulnerability scanning to assess any cybersecurity concerns with regards to our voter registration system. This risk and vulnerability assessment provided my office with areas that needed to be improved upon to ensure our system is as secure as possible. We also looked to the Rhode Island National Guard to provide us with a security analysis of newly-purchased electronic poll books during a recent special election.

Our second challenge is one of building the capacity of the public sector to manage and respond to cyber threats and in our elections. Some of those services can be outsourced. However, we need to make sure that Government owns the ability to protect our democracy. In Rhode Island I have increased my office's I.T. staff by 40 percent to make sure that we have the technical expertise in-house to respond to ever shifting landscape of cybersecurity.

Our work recently received additional help from the Federal level. Working with the National Association of Secretaries of State, the Department of Homeland Security provided—initiated a process for providing two State election officials, like myself, with the required security clearance and this has been really helpful.

At this time I do want to also add my congratulations to Under Secretary Krebs for his appointment, and I also want to recognize the hire at DHS of former Election Assistance Commissioner Chairman, Matt Masterson. I believe that really strengthens the operations and the ability of DHS to work with the States on cybersecurity and elections.

But building the strength of our election system at the State level addresses only part of what is needed. Local election officials are literally on the front lines and must have the information or resources necessary to identify and mitigate the emerging threats.

For this reason, in Rhode Island, we are members of the Election Infrastructure Information Sharing and Analysis Center, the EI-ISAC. Soon all cities and towns in Rhode Island will be signed up with EI-ISAC which provides election officials with cybersecurity resources as well as best practices that enhance the overall strength of election systems.

As cyber threats continue to evolve and become more sophisticated, States need additional funding and resources dedicated to the security of election. These funds have been critically needed for strengthening the I.T. capacity within Government, developing testing procedures, and undergoing third-party assessments.

Our amount of \$3 million is being used to invest in our central voter registration database, strengthening of that system and—as well as protecting it, and other large portions can help us develop our first-ever post-election audit systems in Rhode Island. Finally keeping in mind what I said about local government, we are to be using part of the \$3 million to initiate an election assistance—elections administration improvement grant program for cities and towns.

In conclusion, I want to make the following suggestions. First, Congress should provide on-going funding to the States so that we

remain prepared to face any cybersecurity challenge. Second, Federal agencies must continue to provide information, training, and resources to support the work being done to protect our election systems on a State, county, and local level.

Congress can help us by formalizing clear communication channels between the levels of government so that we know what to expect in the communication of cybersecurity. Finally, Congress must also continue to provide active oversight in this area that now recognizes the new balance that must be struck between the secrecy required for security measures needed to safeguard our democracy at the same time as we balance it with a transparency and access to information that ensure an open government.

Thank you very much for the opportunity to share my thoughts with you on this and my experiences as Rhode Island's secretary of state; I look forward to continuing our conversation.

[The prepared statement of Ms. Gorbea follows:]

PREPARED STATEMENT OF NELLIE M. GORBEA

JULY 11, 2018

Thank you, Chairman McCaul and Members of the committee, for the invitation to participate in this important discussion of how to best address cyber threats to our elections.

I commend your committee for holding this hearing to learn more about what is being done on the Federal, State, and local levels to protect our Nation's elections systems and what can be done to improve upon this work. The advances in technology have brought with them a paradigm shift in elections administration. Addressing cybersecurity in elections has become an urgent and relevant matter. Cybersecurity is at the forefront of elections conversations taking place right now at every level of government across the country.

Before I continue, I want to recognize my Congressman, Jim Langevin, for his visionary leadership in elections administration in his past service as Rhode Island's Secretary of State. Two decades ago, then-Secretary Langevin led Rhode Island's early adoption of voting technology that replaced the ancient mechanical *Shoup Lever* voting machines with paper-based optical scanners.

In Rhode Island, we are proud of our role as an innovator in elections technology. In 1936, for example, Rhode Island was the first State to use voting machines at every polling place across the State, not just in major cities, as had been the practice at that time across the country.

As Secretary of State, I am building on that legacy of innovation and excellence despite the significant challenges that my State and almost all other States face. These challenges can be summarized as follows:

1. First, although this is not currently the case in Rhode Island, many elections across our country are being run on equipment that is either obsolete or near the end of its useful life.
2. Second, our public-sector employees and systems at the State, county, and municipal levels are ill-prepared to handle the looming threat of cyber attacks.
3. Finally, our country is facing a very real threat presented by foreign actors and others who are conducting activities that serve to erode the public's trust in the integrity of our elections. These attacks are real and are focused on undermining our representative democracy.

Congress recently took an important step to help us address these challenges by providing \$380 million for elections administration and security in additional Help America Vote Act (HAVA) funds in the Consolidated Appropriations Act. On behalf of my colleagues who oversee elections across the country I thank you for this important investment. I also want to emphasize that the challenges our democracy faces require an on-going commitment of funds. Elections officials today, are tasked with preparing for threats that were nonexistent 5 years ago and are continuously evolving. Funds, training, and improved communication are critical to ensuring that we continue to protect our democracy.

Actions addressing this new landscape of elections and cybersecurity have taken place in a variety of ways because elections are organized and run differently in every State. Nonetheless, I believe that our efforts in Rhode Island over the past

3 years offer valuable insight into the challenges and opportunities that elections officials face in this era of increased cyber threats.

In Rhode Island, while I serve as chief State election official under HAVA, elections are run in coordination and collaboration between my office, the Rhode Island State Board of Elections, and local elections officials with their boards of canvassers. My office, the Department of State, maintains the Central Voter Registration System (CVRS), a voter registration database and elections management system used by all local elections officials that was developed thanks to HAVA funding during Secretary of State Matthew A. Brown's administration. A separate agency, the Rhode Island State Board of Elections, oversees Election Day operations, is responsible for the security of the voting equipment and handles post-election disputes and audits. Meanwhile, local elections officials and their boards of canvassers run the polls on Election Day.

Our collaboration is a key ingredient to successfully running elections. Over the past year, we have strengthened relationships with our Federal partners, specifically the Election Assistance Commission (EAC) and the Department of Homeland Security (DHS). We have also taken advantage of State resources such as the cyber unit at the Rhode Island National Guard and the expertise of faculty members at Salve Regina University and Brown University.

So how has Rhode Island handled the three challenges I described above?

First, we addressed the topic of equipment. When I took office in 2015, our voting equipment, purchased in 1997, was on the brink of total failure. Thankfully, when I confronted them with the problem, the leadership of our State took this issue seriously—Speaker Nicholas Mattiello, then Senate President Teresa Paiva Weed and the membership of the General Assembly, along with Governor Gina Raimondo, all supported the purchase of new paper-ballot optical scanning machines. This translated into an investment of nearly \$10 million over the next 7 years. The EAC was instrumental in providing us with key advice and counsel in the development of the Request for Proposals for the new voting equipment. Because of these efforts Rhode Island entered the 2016 election cycle with new, secure voting machines that have four layers of security and encryption.

We have also modernized many other aspects of the electoral process and infrastructure. Over the past 2 years we have implemented on-line voter registration, acquired electronic poll books, and recently implemented automated voter registration. These advancements make both voting and the administration of elections more efficient for all involved.

While modernizing the electoral process and infrastructure, we also leveraged resources offered by the Department of Homeland Security under their critical infrastructure designation, to further protect our Central Voter Registration System. Recently, DHS performed external penetration testing and vulnerability scanning to assess any cybersecurity concerns with regard to our voter registration system. This Risk and Vulnerability Assessment provided my office with areas that needed to be improved to ensure our system is as secure as possible. In addition, the Rhode Island National Guard provided a security analysis of the electronic poll books (e-poll books), used during a recent election, to assess possible security vulnerabilities.

But investments in hardware and software cannot be used effectively if government does not have the human resources that can manage and operate them. Our second challenge is one of building the capacity of the public sector to manage and respond to cyber threats in our elections.

In Rhode Island, I have increased my office's IT staff by 40 percent to ensure that we have the technical expertise in-house necessary to respond to the ever-shifting landscape that technology presents. This investment in our State workforce has also allowed us to deploy on-line tools and resources that not only make our elections infrastructure more secure, they make it easier for voters to participate in elections.

It is important to note that security breaches can come through any connection within a governmental office, even those that may be physically removed from elections-related infrastructure. That is why over the past year we have conducted social engineering training, where our own IT team sends phishing emails to employees to test their awareness of potentially harmful emails. In addition, all our employees participated in cybersecurity awareness and threat mitigation training. These tools teach employees about the dangers of methods that on-line hackers commonly use to attempt to infect our network.

However, having technically proficient State and local technology professionals is not enough if we do not have a well-developed communications structure between DHS and our country's chief State election officials. Being able to quickly disseminate information on potential threats and respond effectively is critical to safeguarding our elections. The National Association of Secretaries of State was able to persuasively present this issue to the Department of Homeland Security and, as a

result, DHS initiated the process of providing chief State election officials like myself with the required security clearance to effectively manage the cybersecurity of elections systems. While this process of communicating cyberthreat information between DHS and chief State election officials was admittedly rocky at first, it is now much improved and will be an important mechanism to share cyber threat information. At this time, I would like to commend DHS for bringing on former EAC Chairman Matt Masterson to work with States on cybersecurity issues. In my experience working with former Chairman Masterson I have found him to be a consummate professional, and his thorough knowledge of our country's complex elections systems gives DHS critically important knowledge for more effective policy making.

Additionally, local elections officials are on the front lines and must have the information and resources necessary to identify and mitigate emerging threats. For this reason, in Rhode Island we are members of the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). In addition, by the end of next week I expect all our cities and towns to be signed-up with EI-ISAC. These organizations provide elections officials with cybersecurity products and services as well as best practices that enhance the overall strength of our election systems. For example, the Albert sensor is a device provided by MS-ISAC that monitors and analyzes all traffic that comes into our network. The information it collects is scanned and if something malicious is detected, we are notified.

In Rhode Island, we are also taking steps of our own to ensure full preparedness. Last month, my office and the State Board of Elections hosted a seminar for local elections officials that included a comprehensive tabletop exercise presenting potential scenarios on Election Day. Elections officials were forced to make quick decisions under pressure and practice how to handle such situations. The exercise was based on a similar program my team attended at Harvard University's Belfer Center.

Last year, I convened more than a hundred of Rhode Island's local elections officials and IT staff for a summit on elections cybersecurity. Several industry and academic experts in the field of cybersecurity, as well as Congressman Langevin, provided briefings during the summit. One important message that we focused on that day with local elections officials is that cybersecurity is not a destination; it is a continuous process of assessment, improvement of our systems, and mitigation of risk.

This is why we must bring together all stakeholders, regardless of political affiliations, to continually identify threats and work on solutions. This is not a far-fetched ideal. In fact, IT leaders from Google and Facebook have commented that the top technology companies in our country regularly collaborate on cyberthreat information facing their companies despite being fierce competitors. We must develop a similar protocol in the public sector to share information on cyber threats. In Rhode Island, I have focused on ensuring that our elections officials and staff at every level have the information necessary to minimize cybersecurity threats.

Investment in training of our public-sector employees has become a critical need. As cyber threats continue to evolve and become more sophisticated, States need additional funding and resources dedicated to the security of elections systems. These funds are necessary for third-party assessments, testing procedures, and strengthening IT capacity. The HAVA funds approved by Congress in the recently-passed Appropriations Act are an important initial investment in such systems.

Using Rhode Island as an example, I would like to take a minute to discuss some of the critical initiatives that we are investing in with the new HAVA funds.

- One of our key priorities is to secure the registry of voters. Prior to the 2018 election we plan to invest over \$500,000 in cybersecurity enhancements to our CVRS.
- The new funds also enable us to rewrite our CVRS application, originally developed in 2004 and 2005, to current industry best-practice standards and help us protect against penetration attempts.
- Understanding that trust in elections results is critical, we will fund the first-ever post-election audits in Rhode Island. This law was passed by our legislature in 2017 and is another step in ensuring the integrity of our elections.
- Ensuring that municipalities also improve their systems and help protect our elections, we will initiate an Elections Administration Improvement Grant Program for cities and towns to make election security enhancements on a local level.

In conclusion, I would like to make the following suggestions:

- Congress can play a critical role by providing on-going funding to the States so that we remain prepared to face any cybersecurity challenge. As I mentioned above, the additional HAVA funds approved earlier this year are welcome and much needed by jurisdictions across the country. However, sustained funding is

necessary for elections officials to modernize their systems to enhance the integrity and security of our elections.

- Federal agencies must continue to provide important training and resources to support the work being done on a State and local level to protect our elections systems.
- Congress also can formalize clear communication channels between Federal agencies and State and local governments to share cyber threats and information to assist in preparing for any outside interference in our elections. The Federal Government should recognize that it can play a critical advisory and support role in securing elections infrastructure while respecting the fact that elections are the responsibility of State and local elections officials. It is my firm belief that improving the integrity of elections systems can be achieved while simultaneously improving access to voting.
- Finally, Congress must also provide oversight of Federal intelligence and security agencies recognizing the important balance that must be kept between security measures needed to safeguard our democracy and the transparency and access to information that preserve our ability to have open government and elections that can be trusted.

Thank you again for the opportunity to present testimony on the work we are doing in Rhode Island and how the Federal Government can work with States to ensure our Nation's elections systems are secure and our democracy safeguarded.

Chairman McCAUL. Thank you, Secretary.

I now recognize myself for 5 minutes of questioning. In October 2016, the Ranking Member and I sat in what is called a Gang of Eight briefing with the DNI Director Clapper and Secretary of Homeland Jeh Johnson.

We were briefed at that time, in a Classified setting. Since then, the information has been made public that Russia was attempting to meddle in our elections using a campaign and information warfare model. I would—I would have to say it was very disturbing. I think I speak for the Ranking Member, as well.

I urged, then at that time, that—the previous administration to call out Russia for what they were doing and that there should be consequences to their actions. I have also said the same thing to this administration that Russia needs to be called out and there should be consequences. Congress passed sanctions—harsh sanctions against Russia for their conduct.

With that, Mr. Krebs, I want to ask you if you—as we move into the 2016—or 2018 mid-term elections, can you tell me what the threat level is from foreign adversaries and foreign nation-states to potentially meddle in the upcoming elections?

Under Secretary KREBS. So, as I mentioned in my opening statement, we have not seen anything, certainly, to the degree of 2016 in terms of specific hacking of election systems. I think at this point it is—it is important to—to distinguish or differentiate between directed technical attacks against I.T. systems, much like what we saw in 2016 with the—the database—the voter registration database is the scanning.

That is the cybersecurity technical piece of it. Then, there's also an information operations element of it. I think that is fairly well-characterized in the intelligence community assessment.

We are, again, not seeing, on either hand, something that rises to—anything that rises from—to the level of 2016 directed, focused, robust campaign, but we do see continued Russian activities. The intelligence community continues to see Russian activity in the sowing discord across the American public.

It is not, again, directed, necessarily, at politicians or political campaigns, but it is focused on identifying divisive issues, and sow-

ing discord, and creating chaos, and, frankly, undermining democracy.

Chairman MCCAUL. So there will be more of this campaign information or disinformation warfare?

Under Secretary KREBS. Yes, sir, that is the way I would characterize it. We are seeing more along the lines of information operations rather than directed technical attacks or anything focusing on elections of, particularly, the mid-terms.

Chairman MCCAUL. So, that leads me to the—the vulnerabilities in the election system itself. You don't see any targeted technical attacks toward, say, the voting machines?

Under Secretary KREBS. In terms of the—just stepping back a little bit on the voting machines and I, you now, of course would defer to Secretary GORBEA and what she has seen in Rhode Island, we are—voting systems in and of themselves are systems of systems.

So, we have the voting day which is what people, typically, think of with e-poll books and optical scanning machines or the DREs. Then, you have a broader system that supports the backend, the information management systems that store voter registration. Just like any I.T. system, there—there are going to be vulnerabilities just by the very nature of it.

There are a series of compensating controls even on DREs that can limit risk. Ultimately, what we are looking for, here, is not a 100 percent secure system. Just like any I.T. system, there is no such thing as a secure I.T. system. What we are looking for is resilience in the system.

To think about this, maybe, in a different way is, over the course of the last couple of months through primaries, there have been a number of issues with I.T. systems and California had a voter printout, about 118,000 voters across 1,000 precincts in L.A. County, and then just recently in Maryland, there was an issue with transferring registration information from the DMV to the Secretary of State—State's office.

What we are really seeing there more than anything is that, yes, there are technical challenges, but the way the system is engineered or architected, in part due to work by Congress, and HAVA in particular, is that even if you showed up to vote and your registration had been, whether accidentally or intentionally, deleted from a voter registration file, you have the ability to request a provisional ballot.

So, if, in 2016, when the Russians were in the Illinois State registration database, had they deleted voter registration files, Illinois citizens would have been able to show up. If their information had been deleted, they still would have been able to request a provisional ballot. They would have cast their ballot; it would have been counted as cast. So, this, again, it is not 100 percent security. We are looking to achieve resilience in the system.

Chairman MCCAUL. Secretary, how resilient do you believe the—your State's system is?

Ms. GORBEA. Our system is actually very resilient and I share Under Secretary Krebb's description of what we are looking for is resilience and not foolproof security. So, we have a series of mitigating factors. One is, of course, protecting the systems. Each city and town has its own structures of how to then transfer that infor-

mation to the central—but what Under Secretary Krebs described is, very much, what is happening in Rhode Island today.

In addition, we have been able to leverage resources, not just from the Federal level but for our own National Guard so that we are constantly testing the security of systems at the same time as we, sort-of, think of the what-if. What if something happens?

So, for example, recently we had a mock disaster day with all of the clerks in the cities and towns to try to go through what happens if you show up on Election Day and you discover that there has been some tampering? What would—how would you respond?

We hadn't done that before this year because it hadn't really come up. So, you have to get people at the local and municipal level to start thinking in this way which goes to my point about—

Chairman MCCAUL. My time is, kind-of—

Ms. GORBEA. Oh, sorry.

Chairman MCCAUL. Expired. But I—let me just say, in terms of the voting machines themselves, most of them—these machines are not connected to the internet now. They are disconnected?

Ms. GORBEA. So, the description of whether or not they are connected is an interesting one because that, also, has changed over time. Most machines are individual and there is a modem transmission for some of them, for example, at the end of the day, that transmits the results. But there are back-ups to that and in the case of Rhode Island, the most important back-up, of course, is the paper ballot.

Chairman MCCAUL. But everything is always front-based going back to the premise of my question, you don't see this technical threat currently?

Ms. GORBEA. In terms of the voting systems in Rhode Island, no.

Chairman MCCAUL. From a foreign adversary?

Ms. GORBEA. From foreign adversaries, no. I do think that—I mean we front-loaded our investment into voting machines and that made a big difference in our—

Chairman MCCAUL. And Under Secretary, you and I talked previously about Members of Congress—how—how safe are we from foreign adversary attacks and how—how protected are we on our networks?

Under Secretary KREBS. So everyone has a different model. I think given the sensitivity of the information, the policy shaping that this body engages in, I think that it is safe to say that a foreign adversary from a pure intelligence perspective would probably want to know what you guys are doing on a daily basis, what policies you are driving.

In terms of how you are positioned from a security perspective, I don't have frankly in-depth knowledge of your I.T. systems given the separation of powers but happy to provide a briefing on, in part, best practices, but also work with the CIO. I think we are doing some engagement on how we can collaborate and help Congress secure their networks.

Chairman MCCAUL. I think that would be helpful. I think most Members have no idea how vulnerable they really are to these attacks.

So with that, I recognize the Ranking Member.

Mr. THOMPSON. Yes, I agree with you because we have been in some hearings—some briefings who really laid out some kind-of scary scenarios. Well, you are—you are official now, Mr. Krebs, welcome.

Just from a historical standpoint, how many States have we identified that the Russians did some form of intrusion in the last elections?

Under Secretary KREBS. So when we think back to 2016, there are a couple ways we have to, kind-of, hash out the information it is all based on frankly awareness visibility into activity and infrastructure. So we have thrown around numbers—18 were either accessed or scanned or targeted or 21, whatever it is. Last summer we—we gave 21, when I—that number, 21 that were scanned, that information is based on the telemetry, the visibility into traffic over networks that we had, that, frankly, that we had visibility to last year.

If you were to ask me what I really thought happened, I would suspect, and Jeannette—Assistant Secretary Manfra said this and I believe Secretary Nielsen said this too, I—I would suspect that the Russians probably scanned all 50 States and 5 territories and the District of Columbia. Scanning, it happens every day; it is an automated process. I just again, I think based on the 21 number, that is not what we were able to see. We have better visibility going in to 2018. We basically have—will have access to close to 50 percent of visible—I am sorry, 100 percent visibility into at least the State networks.

Mr. THOMPSON. So is that scanning considered a vulnerability?

Under Secretary KREBS. The scanning is a threat; a vulnerability would reside in the system. The scanning is the actual foreign adversary's actions to look for vulnerabilities.

Mr. THOMPSON. So since whether it is 18, 21 or whatever, how many States have we worked with to identify, help them identify potential threats or whatever?

Under Secretary KREBS. So at this point, sir, we are working with all 50 States. We have all 50 States as members of the Election Infrastructure Information Sharing and Analysis Center. That is since February when we stood up the I-ISAC close to 1,000 total members of the I-ISAC at this point, and that is 50 States plus local jurisdictions, counties, in associations like NAS—

Mr. THOMPSON. So your testimony is that everybody is cooperating?

Under Secretary KREBS. There are levels of cooperation. As always, everybody has different capabilities of the State level and different resourcing as well. But at this moment I can say that all 50 States are participating in the I-ISAC.

Mr. THOMPSON. Explain resourcing.

Under Secretary KREBS. Sir, resourcing would be how they are funded at the State level. You know, Secretary Gorbey is fortunate to have resources provided by the State treasury that she could in 2016, or prior to 2016, replace her outdated equipment. Not all States are similarly resourced and that is going to be a challenge going forward and I think that is probably the greatest opportunity for policy discussion.

Mr. THOMPSON. Madam Secretary, you talked to some of your colleagues around the country I am sure on this. Can you shed a little light on the resourcing?

Ms. GORBEA. Yes, I can absolutely vouch for the fact that the equipment is just the tip of the iceberg; it is the one that is easy to fix quickly, right? Because you know that it is outdated, you know that it is not up to code and you can replace it any time.

I think the second layer of resourcing that is really important is the public sector rank-and-file people who are working in this in Government. We at some point need to invest in making sure that the people at the local level—you can have fabulous resources at the Federal level at DHS, but if they don't have anyone to engage with at the local level on the security on what all of this means, then you are—you are basically going blind.

So I think that there's, it is two-piece; one is the equipment and the other one is the human resources.

Mr. THOMPSON. So we talked a little bit about this re-siloing that is occurring. Give us your opinion about how you see that, pro or con, in terms of the cyber, Under Secretary?

Under Secretary KREBS. Thank you for the question. I think this one's pretty clear. The Homeland Security Act 2003 provided the Secretary of Homeland Security very clear authorities to lead the critical infrastructure protection activities of the—across the Federal Government in coordination with sector-specific agencies, the intelligence community, and law enforcement.

So I think to the extent that we are creating duplicative, whether it is liability protections or information sharing or information—integration centers, I think that is having a negative effect. It is in some cases it could put us into something along the lines of a pre-9/11 position where we don't have that integration.

That is why in my opening statement said several times that DHS is an information and operations integrator. That is our role.

Mr. THOMPSON. Right. So in other words it would make us less secure?

Under Secretary KREBS. That is my belief, yes, sir.

Mr. THOMPSON. Thank you, Mr. Chairman.

Chairman MCCAUL. The gentleman yields back.

The gentleman from New York, Mr. King, is recognized.

Mr. KING. Thank you, Mr. Chairman. I thank both witnesses for testifying here today and Secretary Krebs, I wish you the very best and, Secretary Gorbea, thank you for your efforts in Rhode Island and for working with my good friend Mr. Langevin.

When we talk about cyber activity by the Russians, today we seem to be focusing obviously on the attempts to hack the election systems, but also they have distorted information and attempted to influence people. What is being done in that and who has primary jurisdiction over that?

Under Secretary KREBS. So as I said earlier on, we do look at things that the technical hacking and then the information operations DHS has lead for supporting State and local governments, and the information—or I am sorry—in a hacking space. FBI has lead in countering foreign interference and the—in the information operations space. DHS does support the FBI's efforts as does of course the intelligence community.

Mr. KING. It—do you want to add to that?

Ms. GORBEA. No, I—they really do have the best information on—particularly the information warfare stuff.

Mr. KING. Right, and how's the level of cooperation with the FBI and DHS in that?

Ms. GORBEA. So most recently, we did have a meeting in February with the Office of the Director of National Intelligence, the FBI and Department of Homeland Security that was incredibly helpful to secretaries of state across the country that were altogether for their annual meeting.

That kind of information is—is critical. We can't—part of the challenge here with elections is elections are decentralized. So—and I think we suffered some, you know, beginning stumbling, you know, when all of this came together.

Where a locality was being informed of a potential breach or activities, and the chief State election officials who happened to be secretaries of state didn't know about it. Those—those communication activities between the Federal and the local and the State level, I think have smoothed out considerably over the last several months as we have learned to get along. The other challenge is that as elected officials, we deal in the world of transparency and open government.

Mr. KING. Right.

Ms. GORBEA. DHS works in a very different mode. That is attention that we need to be conscious of and to make sure that we make—we accept the adequate provisions for.

Mr. KING. We also know that Russia is interfering in elections throughout Europe, more elections coming up, more meddling expected. How much information does DHS share with our foreign allies and foreign countries on this and how closely do we work with them?

Under Secretary KREBS. I—it is difficult to quantify how much information we share, but I do know that over the last year or so with various campaigns that happened in Europe, whether it was France or Germany, we do have cert-to-cert relationships, where we can share technical indicators of known command-and-control infrastructure of Russian adversaries.

So we can help them—we will share what we know, they will share what they know, so I do feel as if it is a good relationship in terms of the engagement.

Mr. KING. As far as Rhode Island, you may have covered this in your opening statement but how much cooperation is there among the States as far as, you know, you sitting down with other secretaries of state?

Ms. GORBEA. So the National Association of Secretaries of State provides an excellent coming together on a bipartisan basis so that we can have these conversations about what is happening. We have also under that advocacy—or not—group—bipartisan group have provided a space for our own I.T. officials with our rank-and-file civil servants to be able to have conversations around security issues and what are best practices. Those are critically important in this day and age.

Mr. KING. Without having to name names, are there other secretaries of state who resist this, who feel that this plot is over—you know, threat is overblown?

Ms. GORBEA. No, I don't think that anybody at this point, well, for the most part, I think everybody agrees that there is some level of threat; I think that was made very clear in our security briefing afternoon. There are more tensions around this issue of the communications with the Federal Government and where—and how do we go about finding out what is happening in our own States so that we can help proactively address the issues at a local level.

Mr. KING. Yes.

Secretary, you want to add anything to that?

Under Secretary KREBS. I think that is spot-on, as I mentioned in my opening, everyone understands that the threat is real. The challenge here is, again, goes to the resourcing issue. If I provide information, what can be done about it?

To the point of the Classified information and how we engage, I aim on a daily basis to operate as much in the unclassified space as possible so that the products that I push out are immediately actionable by broad communities. So it doesn't help me if I am—as Secretary Gorbea pointed out, if I am living in a Classified space. That should not be the DHS mission space; we should be managing risk in an unclassified manner that is informed by threat intelligence.

Mr. KING. Secretary Krebs, Gorbea, thank you very much.

I yield back, Mr. Chairman.

Chairman MCCAUL. Gentleman yields.

The gentleman from Rhode Island, Mr. Langevin is recognized.

Mr. LANGEVIN. Thank you, Mr. Chairman, and thank you, Ranking Member Thompson, and to Secretary Krebs and Secretary Gorbea, thank you again for your testimony and all the work that you are doing to enhance election security across the country.

Mr. Krebs, let me start with you. As you know, the 2018 omnibus provided additional HAVA funding for State election officials to better secure their systems in advance of the mid-terms. Do you believe that the States are using these Federal dollars—States using these Federal dollars are making risk-informed decisions on how to spend them?

Under Secretary KREBS. So I do believe that States are using the money in a manner that addresses their threat model, their risks scenario. I would not though assume that all that money is going to replace out-of-date equipment. There are challenges from a procurement perspective; there are also the challenge for it is frankly not enough money to transition that equipment.

What we have done working with States and informed in part by our risk and vulnerability assessments is working with DHS, working with EAC and with the Government Coordinating Council—put together a list of recommended expenditures.

So if you have got this money from the omnibus, the \$380 million a year distribution, here are good ways to spend it. There are things as simple as hiring what we are calling a cyber navigator, someone that actually has cybersecurity expertise that can get out from your State capital and go work with the various counties.

Because that is the real challenge here, is that when you think about across the Nation, there's close to, if not over, 10,000 jurisdictions and there's not enough cybersecurity expertise to go around as it stands, so let's—let's continue to invest in that.

But it is also things like training, exercises, response planning, patching systems, updating operating systems, things like that.

Mr. LANGEVIN. So the list you mentioned certainly is helpful because it is broad; it is not specific to their systems per se. I guess my—what I would ask, would requirements that States conduct risk assessments before using the Federal dollars help to ensure maximum efficacy to improve their cybersecurity posture?

Under Secretary KREBS. So I think that that is certainly something that we would consider, and we of course, offer the risk and vulnerability assessments to the States at this point. We have conducted about 17 of them; we have another one that is in the process.

But absent the other 31 being completed, or 32 being completed, we are taking the lessons learned, the observations from those risk and vulnerability assessments, and we are sharing those broadly through the ISAC and through our day-to-day engagement. So for those States that don't—haven't done an RVA may not want to do an RVA because they have some other capability, we are going ahead and taking the learnings that we got from the RVA that Rhode Island did and we are pushing that out more broadly.

Again, that is what informed the recommended expenditures or the guidance that we developed with the GCC. So that is a good way of—and—and to be clear, that through all of those risks and vulnerability assessments we saw pretty much the same thing: Out-of-date operating systems, patch management challenges, and lack of awareness across staff. These are all things that we can address through, initially, through the—the HAVA money, but then on-going DHS support.

Mr. LANGEVIN. Thank you. I think that some of those things are very helpful. I think that the requirements for risk assessments would be a best way to use the funds, and I will mention that—I want to point out to the Chairman that the bipartisan PAPER Act that I have introduced with Congressman Mark Meadows contains provisions that will require these kinds of assessments, so—

But Secretary Gorbea, in your testimony you spoke about the need for continued cybersecurity training of State and local election officials. So can you elaborate on the nature of the training that is needed, and in particular, about the resources you hope DHS can provide?

Ms. GORBEA. Yes. Yes, so basically, we are only as strong as our weakest link. While I have been able to really improve the—the cybersecurity at our—in the Department of State, truth is, is that elections in Rhode Island are run also at the local boards of canvassers, as well as the State Board of Elections. So what we have encountered is, once you deal with a hardware issue, you have to deal with the people, as well. DHS has been particularly helpful in helping us navigate through all of that.

I also want to give a shout out, though, to the Election Assistance Commission because when we were looking for new voting

equipment, they were there to help us, also, with best practices. I think that is a perfect role for the Federal Government with locals. The locals know, the State people know where their needs are most pressing.

The training that we have done in Rhode Island involves everything from a cyber summit that you participated in about a year ago, where we—where we basically walked through, why are we having these conversations around cybersecurity? For somebody who's a clerk, who's handling everything from fishing licenses, to other types of licenses, to voter registration, it may not be clear to them why they need to be, you know, safeguarding that password for the central voter registration system, where they are in—when they are doing, you know, voter registrations.

So we had a big conversation with the local officials, and which we will continuously do every 6 months, and as part of every single training that we do out of the Department of State to help build that capacity at the local level.

Mr. LANGEVIN. Thank you very much. I know that my time expired. I want to thank you both for your testimony.

Mr. Chairman, I know, as my time is expired, I would like to submit this question for the record: On April 24, Assistant Secretary Jeanette Manfra testified that the surge in risk and vulnerability assessments for election infrastructure created a significant backlog in other critical infrastructure sectors and Federal agencies waiting for similar assessments. The President's 2019 budget did not request an increase in resources sufficient to overcome this backlog.

So my question would be, are—are more resources necessary to support the increased requests from State and local governments without delaying other assessments, or do you expect RVA backlogs to be the new normal at NPPD? I will submit that for the record, since my time is expired.

Thank you, Mr. Chairman.

Chairman MCCAUL. The gentleman yields.

The gentleman from Alabama, Mr. Rogers, is recognized.

Mr. ROGERS. Thank you, Mr. Chairman.

Secretary Krebs, I have been surprised that so many Americans have acted shocked that Russia was meddling in our election, when they have been meddling in elections all across the globe in countries, particularly European countries, and most specifically, Eastern European countries that used to be a part of the USSR, and they do this primarily through disinformation. Many people in America may not realize that R.T. is Russia Today, and it is propaganda too.

My question is, since disinformation is their tool of choice, or their weapon of choice, in meddling in elections across the globe, do you have somebody in your department, or is it your department's job to counter this disinformation when you find it in our country? If not, what department does have that responsibility?

Under Secretary KREBS. So as I mentioned earlier, the way we look at it, again, is the technical hacking piece, and then there's the information operations, DHS leads the cybersecurity working with State and local. FBI leads information operations, but DHS does support. So FBI's role working with the intelligence commu-

nity is identifying specific actors, whether it is Twitter handles or whatever it is, and disrupting those activities.

Now, that is only part of the problem, is actually taking down the disruptive activity, because frankly, with disinformation, the way to counter disinformation is actually shine light on the activity. So what we are doing at DHS working with others in the State Department Global Engagement Center, working with the FBI, is to build a greater understanding and awareness of what their activities are, engaging social media companies, engaging traditional media and sharing our findings, our trends. Here are the things that they are doing. How do we raise awareness across the American public?

This is one of those cases that it is different from traditional cybersecurity, because cybersecurity—elections, for instance. What we are aiming for is resilience in the system so we can take a lick, and we can keep going forward.

Disinformation's completely different. It is—the objective is anti-fragility, and what that means is unlike resilience, where you just want to keep moving through it, with anti-fragility you want to come back stronger; where you learned from the experience, or that engagement, we learned in 2016—that we learned, and we closed out that avenue of influence. That is where we are aiming for.

So we are doing a good bit of trend analysis of how we are seeing Russian actors engage through information campaigns and—and operations, and looking for opportunities of intervention to close out those—those avenues.

Mr. ROGERS. So when you say, “we,” are you talking about just DHS, or—

Under Secretary KREBS. No, sir. It is, it is a whole—it is a cross-government agency. I, in my operation and NPPD, working with the Intelligence Analysis Directorate, the Privacy Office, the Civil Rights and Civil Liberties Office of DHS, among others, we have established a Countering Foreign Influence Task Force, and they—we are looking at some of the—the unique authorities the Department has.

That works in coordination with the FBI's Foreign Influence Task Force, and it is also supported by the intelligence community and the State Department; so it is—everybody has a role in this, given the unique authorities and the, well, frankly, the unique authorities of the various agencies.

Mr. ROGERS. Thank you.

Secretary GORBEA, you talked about replacing all of your voting machines in the State. How much did it cost to do that?

Ms. GORBEA. \$10 million.

Mr. ROGERS. How much of that was State money?

Ms. GORBEA. All of it.

Mr. ROGERS. All of it was State money?

Ms. GORBEA. Yes.

Mr. ROGERS. No Federal money was used?

Ms. GORBEA. No Federal money was used.

Mr. ROGERS. Have you received any Federal money for any security improvements?

Ms. GORBEA. Yes. Well, where we will be using the \$3 million HAVA funds to continue now to really tackle our central voter reg-

istration system, which was developed with, actually, the first batch of HAVA monies. So that application will be rewritten and strengthened.

Mr. ROGERS. Now, you mentioned earlier in your opening statement that you needed to make some improvements to your central database. What exactly are you talking about?

Ms. GORBEA. So just for the protections. You know, our—the focus of our risk vulnerability assessment was actually our central voter registration database, to make sure that we didn't know of open doors throughout our systems that somebody might come in through. So that was—

Mr. ROGERS. Is it connected to a network?

Ms. GORBEA. Yes, and—actually I must say we actually now have trained all of our staff and continue to do on-going training to every—whether you are in the archives of the secretary of state's office or in business services, is to identify phishing e-mails, things like that, so everybody's on their toes to not click on something that might compromise our elections.

Mr. ROGERS. Excellent, thank you very much, thank you all for being here, I yield back.

Chairman MCCAUL. Gentleman yields back, the gentlelady from New Jersey, Mrs. Watson Coleman is recognized.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman. Congratulations to you, Mr. Krebs, and thank you for being here, Madam Secretary. I just—I have got a couple of questions. Is it possible that Russia could be doing something right now that would interfere with this 2018 election and we might not know about it yet?

Could they possibly be involved some way now, or is it just too early?

Mr. KREBS. You know, again, like I mentioned, we haven't seen anything certainly on the level of 2016, neither on the direct hacking. We do know that they are launching—they are carrying out generally speaking information operations.

You know, I—this is kind-of one of those, you know, I don't know what I don't know right now.

Mrs. WATSON COLEMAN. How many months in advance was this hacking identified before the 2016? Was it 3 months before, 2 months before, 5 months before?

Under Secretary KREBS. That was before my time at the Department, I was still in the private sector.

Mrs. WATSON COLEMAN. Would you know, though, this—

Under Secretary KREBS. It was over the course of the summer I believe prior to the 2016.

Mrs. WATSON COLEMAN. OK so it is really this summer that we need—

Under Secretary KREBS. It was—you know, I think the real, as I recall, the real indicators of activity took place about this time July 2016.

Mrs. WATSON COLEMAN. It is really confusing to me, all of the various agencies that are—have a piece of this. So is there like a routine meeting that you all have around these issues?

Under Secretary KREBS. So in terms of the cybersecurity piece, yes, ma'am. We have developed a government coordinating council

that brings not just Federal agencies together, but also State and local partners.

So in that, it is a weekly meeting that DHS, the Election Assistance Commission, but also, you know, I am of the mind that when it is just the Federal Government working together on a problem, you are not getting a lot done because the Federal Government doesn't always have all the answers.

We need to work with our stakeholders, again, as I said in my opening statement, to understand what their requirements are so that we can tailor our services to address their needs. That is really the mantra that I have instituted across NPPD, it is requirements-based.

Mrs. WATSON COLEMAN. Do you think or even do you think, Madam Secretary, based upon your involvement, that all 50 States are equally concerned, engaged, and willing to participate as rigorously as possible to ensure that our infrastructure, voting infrastructure is protected, and our voters votes are counted?

Ms. GORBEA. So I cannot speak for all 50 States, I can tell you that at the National Association of Secretaries of State, these issues have been highlighted and discussed more so than I ever thought when I was running for secretary of state.

Mrs. WATSON COLEMAN. Well, like the President still doesn't believe that this is happening because Vladimir Putin has told him that it hasn't. In your sort-of interactions, are there any States that kind of are where the President is on this, that it really didn't happen, it is crap, or does everyone recognize except for the President that this did happen?

Ms. GORBEA. I personally have not had any conversations that—that way.

Mrs. WATSON COLEMAN. So \$38 million has been appropriated to help various States protect their systems or do whatever they have to do. Does that include money going down into the municipalities and the counties to train people, to do the audits that need to be done, to replace the equipment that needs to be replaced, Mr. Krebs?

Under Secretary KREBS. So the \$380 million in the fiscal year 2018 omnibus is a broad—is available for a broad set of—

Mrs. WATSON COLEMAN. But it can—it goes to the States and then the States will decide how to spend it?

Under Secretary KREBS. I believe that is correct—

Ms. GORBEA. That is correct, and it is—there is actually a fair—while there are guidance and sort-of big buckets of categories, it is really allowed—it really allows the chief State election official to allocate it in the best way possible—

Mrs. WATSON COLEMAN. So it is been indicated that the States have suggested a \$380 million, while a lot of money is not adequate. Do you have any idea what that number should be, from their perspective?

Ms. GORBEA. Not—not off-hand, although I can use Rhode Island as an example for exempt. So we are receiving \$3 million, our replacement alone, voting systems of the machines, was \$10 million.

Mrs. WATSON COLEMAN. That was purely State money.

Ms. GORBEA. That is right.

Mrs. WATSON COLEMAN. So if a State doesn't have it, and this \$380 million could be legitimately used for it, it seems like it really could be a lot more depending upon how many States have the capacity to do this and want to do it.

Ms. GORBEA. Yes, that is correct.

Mrs. WATSON COLEMAN. OK, thank you, thank you, I yield back. Thank you, Mr. Chair.

Chairman McCAUL. The gentlelady yields, the gentleman from Pennsylvania, Mr. Perry is recognized.

Mr. PERRY. Thanks, Mr. Chairman, and congratulations, Secretary, and welcome, Madam Secretary, appreciate your presence. I just want to make sure I understand the playing field in—in the context that Russia or the USSR in its previous version has been involved in the United States and undermining the United States since 1917, since the Bolshevik revolution.

I mean, and the history of the Venona transcripts and receipts show that they infiltrated our Government at the very, very highest levels and influence policy in magnificent effect in the decades past.

But under—so this is nothing new, but in the current context, Madam Secretary, in particular, do we know of—and, Secretary, if you know, their incursion into the most recent Federal election, the Presidential election, they didn't change any of the votes as far as I know, right.

We are talking about information gathering and—but I think in the greater sense, they are—we are talking about propaganda and influence operations as opposed to vote tampering or changing. Am I correct in that assessment?

Under Secretary KREBS. So from the extent of our understanding in 2016—rather, the extent of their access was to voter registration database that was not a vote count, it was well kind-of left of voting day. So they were able to get into a State voter registration database and exfiltrate some data.

Mr. PERRY. Their interest in looking at the voter database so to speak was to then provide propaganda or information to key voters or to target—

Under Secretary KREBS. I am not actually sure that is—that that was their intent. In fact, I think to a certain extent, they didn't know necessarily what they were looking at. They were in a certain—to a certain—perhaps mucking around in a system, trying to figure out where they had landed and where they were.

And understand frankly how the systems worked and how they interoperated. But to be clear, we did not see them having access to any machines, equipment, or whatever that was involved in voter—vote tallying.

Mr. PERRY. It is because of the lack of network access and decentralization of the voting system among States that even if they would have wanted to, they figured out where they were and they wanted to influence I would have been very, very difficult.

That is my understanding, but I want to clarify that, or have you—

Under Secretary KREBS. That is certainly a contributing factor, yes sir.

Secretary PERRY. OK, and so at this point other than access to voter registration, we don't know what their intent was and they don't at this point admit that they were ever even involved right? They still don't admit that they were ever involved but we are fairly confident that they were. Is that correct?

Under Secretary KREBS. The intelligence community assessment from 2017 was pretty clear that they did intend to interfere, yes sir.

Mr. PERRY. But we don't know in what way they—

Under Secretary KREBS. In what way, I would have to go back and do a dig back into the ICA, but—

Mr. PERRY. OK. I think that is important to know to inform us of future elections. I don't suspect since they deny currently that they were even involved, that they will ever admit that they are probably going to try to stay involved and continue to be involved as they have since for the last 100 years essentially. Right? They are probably going to—so it would be important to know I would think to get an assessment of what they were seeking to do if they did in fact get in. We should know that so we could safeguard in the future.

But let us go to the Countering Foreign Influence Task Force that you talked about regarding propaganda and disinformation. We have got an election coming up in about 4 months. Will that organization be prepared at that time to inform, by whatever method it decides and determines is appropriate, the American public of things like Russia today or ads on social media, etcetera to influence, via propaganda, the American electorate? Will that task force be prepared at that time to be engaged?

Under Secretary KREBS. Some of my task force I wouldn't think of it as an incident response capability, I think of it more as an analytical cell. See what the activities they do over time, what their tactics, techniques, and procedures are and build up a body of knowledge to then share generally speaking. Here are the sorts of things they do. These are the sorts of things that the American public should be on the lookout for. Other agencies have the more tactical response of we are seeing, for instance, the Internet Research Agency perhaps do activity X, Y, or Z, that is where the FBI becomes involved; that is where other agencies become involved, it is more tactical—

Mr. PERRY. OK so I think I have a clear understanding of that but what I am missing and I think some other Members might be missing is once we have that information, once we have that track record, then what? Who is going to inform the American people of this advertisement is specifically coming from a propaganda source whether it is Russia or some other hostile Nation or adversarial Nation and to be suspicious of it. Whose job in the American—in the Federal Government or State and local governments is it to do that informing of the citizenry?

Under Secretary KREBS. So this is in part a Government and industry collaboration. So where we have social media companies working with Government we will be able to identify that information whether to flag it or take it down similar to terrorists use the internet where they remove content, disable accounts, that sort of

activity can happen on the private-sector side and on the industry side.

Mr. PERRY. So it is planned solely on the private sector?

Under Secretary KREBS. No sir, it is—this is truly a partnership. This is going to be the Government will be taking certain actions then the private sector will be taking certain actions. I think if you look at what Twitter has done over the last week or so or last month, couple months, where they have disabled 70 million accounts by press reports at least. I think that is the sort of activity you will see happening going forward.

Mr. PERRY. OK, thanks Mr. Chairman I yield.

Chairman MCCAUL. The gentleman yields. The gentlelady from Florida, Mrs. Demings is recognized.

Mrs. DEMINGS. Thank you so much Mr. Chairman and thank you to both of you for being here with us today. Congratulations, Mr. Under Secretary, and thank you so much for the work that you are doing in Rhode Island as well.

Let me just say I—we have heard a lot about what happened in 2016 with our election and I grew up in Florida and Florida is the State that kind of keeps everyone up all night, especially on general election night. I just, I think everybody here understands the importance of protecting our systems but let me just say this. I grew up in Florida. I represent a district in Florida.

When I think about my parents, my mother was a maid and my father was a janitor, but I cannot remember a time they did not exercise their right to vote and I think they were so dedicated because they understood that regardless of the color of their skin or where they lived or how much money they did not have in the bank that their vote mattered, it counted and it counted as much as any billionaire or millionaire in this country. So why wouldn't we especially, as one of the most powerful bodies in the world, in Congress want to protect this basic right for every American?

So I do thank you for the work that you are doing to further that goal. Under Secretary, I was a little bit surprised as we look at I think the viciousness and consistency of Russia and other foreign powers that want to attack our system, that more States had not taken advantage of the full array of resources that DHS offers.

I know that—I believe you said 17 have participated in the risk vulnerability assessments. When we think about—a No. 1, I would like to know, what you think you could do to encourage more States to participate, even though it is that they have the option the ability to opt in or not and also for State like Florida, if they did today call and say they want the vulnerability risk assessment done, how soon could you get that done?

Under Secretary KREBS. So to your first question, what can we do more of? We need to continue steady-state engagement working through a number of different venues like the National Association of Secretaries of State has been a huge partner amplifying our message. But it is also important to understand that that the DHS service of the risk and vulnerability assessment is just one of several options that States have available.

We have approached some States. They have said thank you for the offer but we have a private-sector solution that does exactly that, that is already on contract, so I don't ever frankly anticipate

getting all 50 States in the risk and vulnerability assessment process. I suspect we maybe get the 25 maybe 30 that is kind-of a stretch. It is, for us, again, it is reaching out, continuing the engagement, continuing the education and really frankly more than anything, it is building a relationship and building and establishing trust.

We are still getting, you know, I think for the most part we have gotten over kind-of the trust hump that we—the challenge that we had last year, I think we are getting there.

So in terms of Florida, or frankly any State that was to ask for a risk and vulnerability assessment, we have been very clear in how we have communicated to our State partners that as soon as you are ready to do a risk and vulnerability assessment, we will be there.

There were discussions last time, I think I testified about a 9-month backlog. There's no 9-month backlog, it is when the State is available to do it and it is not just show up tomorrow and we will do a vulnerability assessment. There is a little bit of preparation that has to happen. I am sure Secretary Gorbea can share her experience, but there is preparation that has to happen before we can go in there and do our penetration testing. There are legal agreements that have to be signed. There's scoping of the networks that we have to do. So there are a number of preparatory measures that do lead to some time buffer before we can actually get in there.

Mrs. DEMINGS. Thank you. Secretary Gorbea.

Ms. GORBEA. No, I have to say, you know, on the ground, we have found DHS to be actually very responsive. In fact, one of the first things that they—we were probably one of the first to sign up for the—under the critical infrastructure set-up.

Then, the next thing I remember, we had, you know, three people showed up in my office and the regional director, a program person, a security person all introduced themselves, in person. Which I have to say is, probably, on the first times I have seen anybody from the Federal Government, you know, sort-of, show up in my office and introduced themselves to my staff.

So, that created a bond in terms of a trust factor because I know who I am dealing with and that started our process going and we did do the risk and vulnerability assessment. What I think, then, what was interesting is to see the disconnect, sort-of, in a broader basis as information at the very, sort-of, in the Classified and intelligence level, sort-of, started to happen.

There were some misfires in terms of, you know, they would contact the locality, but not the chief State election official. If you are a chief State election official and you are also an elected, you want to know what is going on in your State, of course. That was, I think, really just this is all new territory for all of us.

We are learning cyber stuff, they are learning election stuff and I think one of the really big questions, as this evolves, is that balance between, you know, the security world deals with securing everything down. They don't want to tell, you know, they want to tell as few people as possible.

We deal in the world of open government and transparency. We need to be transparent. Going back to the point that was made ear-

lier, people can—need to be able to trust their elections and so they do that because we are open and transparent in the way we do things.

That is, I think, at the intersection of where the challenge is. How do we secure the elections while not losing the democracy and the secrecy of it all? Because I can't tell you what is happening, but just trust me. Well, no, that is not going to work in the elections frame.

Mrs. DEMINGS. Thank you, so much. Mr. Chairman, I yield back.

Chairman McCAUL. The gentlelady yields. The gentlelady from Arizona, Ms. McSally, is recognized.

Ms. MCSALLY. Thank you, Mr. Chairman. Thanks for your testimony today. Look, we know bad actors like Russia have been trying to undermine our way of life, our representative government. Since the days that I was at the Air Force Academy in the mid-1980's, we have been studying their tactics and they evolve over time, but it is still the same intent.

I really appreciate the discussion today. I think it is really important. I want to talk about the cybersecurity side of this, not the misinformation side and one of those States that was hacked was Arizona, I represent southern Arizona. We have had a Classified briefing on this, but as you talked about, you want to be in the unclassified realm as much as possible.

There are all sorts of media reports out there, but what can you talk about, Under Secretary Krebs, in this open forum, about what happened in Arizona? I know you weren't there, but what your organization knows about what happened in Arizona, when, how it was detected, who was informed, what was learned from it and, you know, the lessons learned going forward? I just think it—there is a lot of confusion in the media and it will be helpful to clear that up.

Under Secretary KREBS. So, thank you for the question and I will go ahead and offer off at the beginning that we come in and provide a bit more of a detailed conversation for you. In fact, for Arizona, it is one of the more challenging situations because it wasn't, necessarily, related directly to Russian activity.

There—secretaries of state, election officials, by their very nature are natural risk managers. They deal with hurricanes, power outages, civil unrest, and criminals that want to get access to personally identifiable information that may reside within voter registration databases. So, every attack, particularly those that we—or incident that we have seen over the last couple of months, even, it is not always Russia.

That is one of the unfortunate aspects of the climate, right now, is that every time you see some sort of disruption, whether it is intentional, malicious, accidental, everyone is jumping to the conclusion of it is Russia. There are things that happen on a daily basis in elections that just happen, so.

Ms. MCSALLY. So, in Arizona can—can you just be clearer? I mean, and by the way, and Russia, criminal elements are often acting on behalf of the States.

Under Secretary KREBS. Yes ma'am.

Ms. MCSALLY. So, let's not be fooled—

Under Secretary KREBS. But we do have criminals here in the United States as well. So, at this point, given the kind of confidential nature of some of these conversations, I can't get too much into the Arizona piece. But again, I would like to follow up with your office on that and see——

Ms. MCSALLY. Yes.

Secretary KREBS [continuing]. And provide you a little bit more information.

Ms. MCSALLY. I would like to let, again, the key of openness and transparency, so people understand. It can help build their faith in the system that nothing was manipulated, but what has been learned from it and what are we doing going forward?

Under Secretary KREBS. Yes, ma'am.

Ms. MCSALLY. Again, we understand that in all the hacks that did happen, nothing was manipulated. But it doesn't mean it couldn't have been manipulated. Just because it hasn't happened, yet, in 2018 doesn't mean it can't happen between now and Election Day. If they choose to, right? Threat equals capability plus intent.

Even though someone can cast a provisional ballot if a zip code was turned around and jumbled up or their street address, if we don't know that that happened then the provisional ballot will be thrown out. Or if their voter file was deleted, they will cast a provisional ballot, it will be compared, and they say it is not a voter and it will be thrown out.

So, just the, you know, I have a concern about the detection and the swift capability, moving forward, for this election and beyond because on Election Day, if the lines are getting longer and people are hearing something's not right. That, in and of itself, meets the intent of the enemy, right? That they are sowing confusion and discord, so can you just talk little bit about that? Because, again, just because they haven't done it yet doesn't mean they can't do it tomorrow.

Under Secretary KREBS. That is 100 percent right. That is why we are not, necessarily, looking back at specifics. We are looking back at the specifics of 2016, but given our broader understanding of the I.T. environments that support elections, we are looking at, more broadly, where the vulnerabilities are, just in the system in general and what are the things we can do to address those vulnerabilities, broadly?

It is not just Arizona. It is obviously all 50 States. So, the thing that I reiterate is we are seeing, as I have traveled across the country through primary season, I am continually impressed by the level of seriousness that secretaries of state and State election directors are paying to this issue. They want more information. They want more threat information. They want more information about how they can understand and manage their risk.

Ms. MCSALLY. Great, thanks. Look, we manage all those at the county level. We do have our secretary of state role as well. We are from Arizona. We are, generally, skeptical of the Federal Government being involved in anything.

We are, you know, we are very independent-minded. So, is—how is your relationship, you know, with the State there and—and the

understanding of the role that you have while still allowing this to be localized and distributed which is where it belongs?

Under Secretary KREBS. So, we do have a relationship with Arizona. We are engaging on a regular basis, I think, as I mentioned they are a member of the Election Infrastructure ISAC. Every State is different. Every architect of a system is different. The threat model is going to be different. Arizona is different than Rhode Island, so.

Ms. MCSALLY. I look forward to following up with you. My time is—

Under Secretary KREBS. Yes, ma'am.

Ms. MCSALLY. Expired, but, specifically, thanks a lot, appreciate it. I yield back.

Chairman MCCAUL. The gentlelady yields the gentlelady from New York, Miss Rice, is recognized.

Miss RICE. Thank you, Mr. Chairman. Mr. Krebs, last week the Senate Intelligence Committee issued a bipartisan report that concurred with the intelligence community's January 2017 assessment that the Russian government interfered in the 2016 election to support the Trump campaign. Do you agree with the Senate Intelligence Committee and the intelligence community's assessment?

Under Secretary KREBS. Yes, ma'am.

Miss RICE. Have you shared your opinion with the President?

Under Secretary KREBS. I have not had the opportunity to meet with the President, directly, about this issue. I have been in briefings with the President on this issue, but I have not directly engaged him on—on that.

Miss RICE. Do you think that this is an important enough issue to engage him on this issue? Since he has repeatedly refused to accept the conclusion of his own intelligence community?

Mr. KREB. Ma'am, residing within a technical agency where I do at the under secretary level, I am not often afforded the opportunity to meet with the President. I don't say this jokingly, it is that I, you know, engage on a daily basis with—

Miss RICE. Have you spoken to the Secretary and suggested to her that she speak directly to the President—

Mr. KREB. Yes, ma'am. We—I meet with the Secretary regularly on this issue, and she has directly briefed the President on this issue.

Miss RICE. The Justice Department and Special Counsel Robert Mueller charged 13 Russian nationals and 3 Russian companies in February with various crimes related to interfering in the 2016 election, including stealing the identities of American citizens. Do you believe that Special Counsel Mueller's investigation is a witch hunt?

Secretary KREB. Ma'am, can you repeat the question? I am trying to understand.

Miss RICE. Yes, I will. The Justice Department and Special Counsel Robert Mueller charged 13 Russian nationals and 3 Russian companies in February with various crimes related to interfering in the 2016 election, which is what we have been talking about here, including stealing the identities of American citizens.

Do you believe that Special Counsel Mueller's investigation is a witch hunt? Yes or no.

Secretary KREB. I certainly don't think that charging the Internet Research Agency and those that supported interfering with the election a witch hunt, no, ma'am.

Miss RICE. So that is a no, you do not believe it is a witch hunt.

Secretary KREB. The 13 indictments you just indicated, I do not believe that those are witch hunts. I think those are legitimate.

Miss RICE. Mueller's investigation into at least that portion of it, you are saying is—

Secretary KREB. Yes, ma'am. I am not aware of the rest of the investigation.

Miss RICE. Do you think the overall investigation is a witch hunt?

Secretary KREB. Ma'am, I am not aware of the scope and extent of the investigation again, I engage every day with State and local election officials on securing their systems, I—you know, I read what I can in the paper, I am not privy to Special Council Mueller's investigation and the scope of it.

Miss RICE. Well, in your position, you should know than more than you are at least attributing yourself knowledge of. Will President Trump be discussing Russian interference in the 2016 election in his meeting with President Vladimir Putin next week?

Secretary KREB. Based on the press reports that I have seen, yes, ma'am, that is part of the agenda.

Miss RICE. Well I would assume that before that meeting, the President is going to sit down with his top people, one of whom is your boss, Secretary Nielsen. Will you recommend to Secretary Nielsen since you don't get direct face time I guess to talk to the President, will you be recommending to her that she recommend to the President that he discussed Russian interference in U.S. elections with President Putin?

Secretary KREB. Again, based on press reports, that will be part of the conversation. Of course I would suggest if I had that conversation with the Secretary—

Miss RICE. Do you think you should have that conversation with her?

Secretary KREB. Again, I speak to the Secretary about this matter on almost a daily basis and we have encouraged it.

Miss RICE. Have you specifically about this issue that I am asking you about, whether she is going to recommend as one of his advisors that he should bring this up in a serious manner with President Putin?

Secretary KREB. I would recommend that, yes, ma'am.

Miss RICE. OK, so just a clarification, why DHS countering foreign influence task force, how it is different from the FBI foreign influence task force, we can debate that all day long.

But why is there not just one comprehensive task force on this critical issue?

Secretary KREB. So I think the challenge here is that from an information operations perspective of what Russia has launched over the last couple years, the Government is not necessarily directly organized from a—there's no single set of jurisdictions, frankly; these issues like the FBI's law enforcement authorities, my authorities to meet with private-sector companies and build awareness and resilience within the system.

We are working toward something like you are suggesting, whether it is a single task force, but we do coordinate on a regular basis. I meet at the under secretary level on an almost weekly basis with my counterparts and a number of different agencies, there are meetings in the National Security Council, and there's staff technical level meetings between DHS, the FBI, the Global Engagement Center.

Miss RICE. Thank you, I yield back, Mr. Chairman.

Chairman MCCAUL. Gentlelady yields, the—let us see, gentleman from Nebraska, Mr. Bacon.

Mr. BACON. Thank you, Mr. Chairman, and I thank you both for being here today. I just want to ask Under Secretary Krebs a—question for clarity. I think you have been touching on it a little bit, I just want to make sure we have it right.

Is there anything else you need from Congress, whether it is resources, the—you know, a budget, the appropriations and so forth, is there anything else you need from us to safeguard our elections systems from hacking or manipulation?

Under Secretary KREBS. So I think from a—thank you for the question. I think from a pure authorities perspective, I think we have everything we need to support State and local governments in their election.

I think with more, from a resourcing perspective, I could always do more. But we are learning from our past engagements, whether it is risk and vulnerability assessments or some of the other capabilities that we are providing.

The \$26.2 million we were providing in the omnibus—the fiscal year 2018 omnibus, certainly helped increase our bandwidth, not just for election systems, but also in those other infrastructure sectors that Congressman Langevin mentioned.

So we are always looking at how to be more efficient in the things we do and make sure that we are operating off of requirements. The last thing I would add on that front is given the nature of a public-private partnership, everything has to be based on the demand signal as we are calling it.

The relationship, frankly, between State officials has only really been at what I would say a healthy level for not even a year now, maybe about a year now. It is still—we are still defining what the requirement sets are, and that is going to be something over the next 6 months, particularly in kind-of the hot wash after 2018, we will get back to—we will pause, reflect, do a hot wash, figure out where we need to go going forward.

Mr. BACON. One of the problems we hear is that our State and local officials don't have the right clearances to work with some of these things. Are we getting that problem solved? Are we making progress?

Under Secretary KREBS. We are, we have taken a pretty hard look at the clearance process. I think at this point we have got about 37 States that have a senior election official with a clearance, 9 more are in the processing, a handful have declined for whatever reason, and they may have other officials in the State that have access to the information.

Others are still in the decision-making process. Very—it is a limited number. But I will also kind-of pull back on the clearance

piece a little bit. As I mentioned earlier, we are doing everything possible we can to take things or to operate in the unclassified space.

I would also suggest that the Classified information piece and the clearance issue is not necessarily the driving factor for our engagements. In a year-and-a-half ago or in 2016, having never met Secretary Gorbea, if I would called her up and said you need to take care of this system right now, she would have said I don't know who you are, I am not going to do that. I have no reason to trust you. Now, if I called her up and said hey, look, we are seeing something, you need to take care of this problem, based on the trust and the relationship we have developed, even without a clearance I have fairly good confidence that Secretary Gorbea would at least give me a flier and then we would follow up afterwards.

Mr. BACON. One last question here, we are seeing more and more attacks from Russia against Ukraine's critical infrastructure, and it seems to me they are using it as a test to practice their techniques and capabilities.

First of all would you agree with that and second, what are we learning from watching what Russia is doing with Ukraine? Because clearly those same capabilities they are using—they are studying us to the same if they need to.

Under Secretary KREBS. I think that is a fair assessment that Ukraine is perhaps a pilot or a test bed. In terms of what we are learning, they are getting better. You know each subsequent incident shows that increased level of capability. So what we are doing is sitting back and looking at, OK, what is the capability that they have demonstrated and what are the corresponding vulnerabilities or exposure or risk level here in the United States and then how do we work with our critical infrastructure community to help them understand that risk and do the things they need to do and how can we help them understand that risk and do the things they need to do and how can we help them do that?

One of the things that I think I—we need to move beyond information sharing. Information sharing is the foundation of how you manage risk. We need to do and continue move into is a risk management integration space. This is the importance of avoiding the silos because increasingly these systems, whether it is industrial control systems, or just general I.T. systems, are almost agnostic to sectors, or at least they cut across several sectors.

So we need to be working cross-sector government industry together to do integrated risk assessments, integrated strategic planning, and integrated risk mitigation strategy. So there is a lot more ahead of us and this is one things were really focusing on right now at NPPD.

Mr. BACON. Thank you very much. Mr. Chairman, I yield back.

Chairman MCCAUL. The gentleman yields back. The gentleman from California, Mr. Correa, is recognized.

Mr. CORREA. Thank you Mr. Chairman. First of all Honorable Krebs, Honorable Gorbea, I want to thank you for being here today and I also want to thank you for the good job you are doing. I know sometimes it goes unappreciated, but we are relying on you, OK?

I wanted to follow up, on it on this committee we talk about best practices when it comes to cybersecurity, financial institutions, I

would presume that right now cross the 50 States, we have some kind of semblance of coordination were those best practices are being applied at every one of those 50 States when it comes to the elections?

Under Secretary KREBS. Yes sir through the Election Infrastructure Information Sharing and Analysis Center. Basically, to kind of unpack what that means is it is a group of all 50 States including other election officials that are connected in a manner that if one has a best practice or an observation they want to share then all 50 are all—

Mr. CORREA. What about in a situation where we have had recently that you have a cyber attack on financial institutions within nano seconds everybody is on top of it so that people figure out that there's actually an attack going on and people can respond to it.

Under Secretary KREBS. Let me actually give you a practical example from the election community.

Mr. CORREA. Yes, sir.

Under Secretary KREBS. A few months ago, there was a phishing attack not necessarily attributed to a nation-state, but a phishing attack on the State election system. What happened is that State detected the phishing attack, worked with DHS, and then we were able to share indicators across the EI-ISAC. Now, did this happen in a matter of seconds or even minutes, no. But what we gain through this approach of community or collective defense is broader community—

Mr. CORREA. Will you be able to get to get there eventually? I know there are a lot of issues, costs, software, hardware, will you be able to get to that level when you have an attack you are able to respond almost immediately?

Under Secretary KREBS. I think ultimately that is our aspiration of course.

Mr. CORREA. I ask that question following up Ms. McSally's point which is trust. I am from the State of California. We are like Arizona, we mistrust the Federal Government, but we try to work with the Federal Government. Yet, really in these elections, the issue is trust. If you wake up Wednesday morning and somebody fried your software system and there are questions of the validity of those election results, we are going to have major challenges to our democracy in this country.

You know I am trying to—in my mind trying to figure out what can we do to help you to make sure that that is not a reality one of these Wednesday mornings?

Ms. GORBEA. Sir if I may—

Mr. CORREA. Yes.

Ms. GORBEA. From the State level, so I think it is this risk mitigation right. We can't just rely on we are going to put a wall around our systems and that is to protect us from everything.

Mr. CORREA. That comes back to the issue of ultimately you come back to paper ballots as being—

Ms. GORBEA. Paper ballots are absolutely critical in my opinion. People ask me all the time, do you think on-line voting should happen? I am like no not really because I for one, even though despite—

Mr. CORREA. Most of the folks I know that show up to California to vote actually vote electronically.

Ms. GORBEA. So I know that California is a very large State with many different systems—

Mr. CORREA. Yes, yes.

Ms. GORBEA. I know that Secretary Padilla has been doing a fantastic job.

Mr. CORREA. I will let him know you said that.

Ms. GORBEA. But going back to—we talked about provisional ballots for example, right. So say something happens and you show up and your name is not on the voter registry, that is as important in my mind to look at what is our provisional balloting system as it is what the machines are, because the machines are, in a sense, easy. You can come in, you can buy them, you put them, you install them, but then what if they don't work? What if somebody sabotages them? What is that next step? We have very different provisional ballot systems in this country. In Rhode Island that is a very simple process—

Mr. CORREA. Do you think that is a formula for major chaos one of these Wednesday mornings that everybody has their own different way of doing it? This is State of Florida, hanging chads all over again.

Ms. GORBEA. I think it is worth examining it. I understand that given—that while—

Mr. CORREA. I only have 40 seconds left. I just want to be quick here but I would like to talk to you a little bit more on this. I used to chair elections when I was in the State senate in California so we dealt with these issues a little bit. Not to the extent we are dealing with them now but my final question and this is one for you maybe to answer or not to answer for us here. At what point does a foreign nation's interference in our electoral system constitute a declaration of war in our country?

Under Secretary KREBS. I think that is the right policy question we need to have right now. I don't have an answer for you.

Ms. GORBEA. I agree. I think that is one of the critical questions we need to ask.

Mr. CORREA. Thank you very much. Mr. Chair, I yield.

Chairman MCCAUL. The gentleman yields, and I appreciate that question. We have been trying to define that for quite some time. Was it an act of cyber warfare? I appreciate you raising that.

The gentleman from New York, Mr. Donovan.

Mr. DONOVAN. I am your last questioner.

Chairman MCCAUL. At least on this side.

Mr. DONOVAN. Yes. The title of the hearing was "DHS's Progress in Securing Election Systems and Other Critical Infrastructure." I would just like to ask about the other critical infrastructure for a moment, since you are both here. Secretary GORBEA, you said before in your opening statement about balancing our needs for secrecy with our need for transparency, a very difficult thing to do.

Mr. Krebs, during, you know some of the other attacks that we have seen on our health care systems, our dams, our oil and natural gas systems, the cyber attacks on our energy industries, how do we balance that need for secrecy and transparency and how do we as a Government share vulnerabilities with private industry?

We all have this same common goal here is to protect our energy system, our electrical grids.

But then, again, there is a difficulty, I suspect, with industry, particularly those who have competitors, of revealing that they are vulnerable. They don't want to lose the confidence of their clients or their users.

So how do we balance that stuff? I know it is not an easy question and there's not an easy answer for that, but since I am the last one on this side of the aisle, I will throw you a hardball.

Under Secretary KREBS. That is a——

Mr. DONOVAN. Thanks.

[Laughter.]

Under Secretary KREBS. That is a great question. The way I kind-of break this up, right now, at least, is to look at opportunistic attacks and then more strategic adversary attacks. So when you think about what happened last summer or last fall with WannaCry, the United States was generally not terribly affected, unlike some of our European counterparts, and look at what happened in Russia and elsewhere.

The reason for that was, in part, because we did a fairly good job, I think, in a Government-industry partnership, of sharing information, indicators, working with the security research community to see what they saw. Then there were some security researchers that took certain activities to help out. But it started before WannaCry even launched, in that we had raised the level of awareness, we would worked with, whether it was the Government doing it, or just in general, the level of awareness, people had done the right cyber hygiene basics to protect their systems.

They had patched their operating systems, they had patched their software, so that the majority of the vulnerabilities had been closed down. So from an opportunistic perspective, I think we are—we are certainly making progress; we are improving.

Now, this is always a question of resourcing; I have said that before today. When we think about the recent rash of ransomware attacks, those are similarly opportunistic attacks—Colorado, Atlanta, Baltimore, Mecklenburg County, Charlotte—those were all attacks that had been, you know, they were scanned, their systems were scanned, they found vulnerabilities, they went in, locked them up and said, “I want \$50,000.”

That is an example of not necessarily doing the basics. So we are really stressing to prevent opportunistic attacks, which is, generally speaking, about 85 percent of, these are, you know, soft numbers, not empirically based but good enough to go by for the purposes of this discussion of, you do the basics right, and you can drive most of the bad actors out of the space, the general hackers.

Now, from a strategic perspective, we do know, as I talked with Congressman Bacon earlier, we do know that the adversary's getting better, particularly in our hard infrastructure space. We saw them last summer, we released a report earlier this year, along with the FBI, on Russian activity in infrastructure. We saw them in energy, critical manufacturing, transportation, aviation.

We are currently seeing them, presently, in the information technology side, the I.T. side. Now, the problem is, once they get more

comfortable operating in the operational technology side. So that is where we are focusing right now.

I mentioned earlier, we talked about siloing, we talked about this shift from information sharing to risk management. That is where we are driving a great deal of our effort right now. It is taking a piece of threat intelligence, like, I know the amount of intelligence I see on a daily basis, it is overwhelming, but what—I need to do a better job of working with industry and saying, this piece of intelligence, so what? What does it mean? What does it mean to that system, this system, to the Nation, to a region?

Figuring that piece out and then asking the question, what are we going to do about it? That is principally where we are focused, and we are kicking off a new initiative within NPPD, the National Risk Management Initiative, that is really going to focus in on moving beyond intelligence and into risk management. Of understanding what the problem is, how to address it and doing it in a cross-sector Government-industry partnership manner. I think that is where we are going to make the most significant gain.

Mr. DONOVAN. You are right. I thank you both for your service. I yield, Mr. Chairman.

Chairman MCCAUL. The gentleman yields.

The gentlelady from California, Ms. Barragán, is recognized.

Ms. BARRAGÁN. Thank you, Mr. Chairman, and thank you both for being here today.

Secretary Krebs, I wanted to ask, last month, I believe, the Senate Intelligence Committee had put out a report called, “Russia Targeting of Election Infrastructure During the 2016 Election.” I assume you have seen that?

Under Secretary KREBS. Yes, ma’am.

Ms. BARRAGÁN. In that report, there was a paragraph, a sentence that said, “although the DHS provided warning to I.T. staff in the fall of 2016, notifications to State election officials were delayed by nearly a year.” That is pretty startling to read, and I think I hear from local elected officials, that is concerning that the Federal Government knew of something yet they didn’t get notice of it. I think I read about North Carolina having problems on election day, and them having no idea about the possible breaches and concerns that were happening. What are you doing to make sure that doesn’t happen again?

Under Secretary KREBS. So on the top end, we have established a series of information-sharing protocols, working with the Government Coordinating Counsel to say, hey, when we get something or we see something, these are the five officials in each State and the system owner that we would notify.

Secretary GORBEA mentioned it earlier, you know, a year ago or even before that, they were trying to figure out the cybersecurity side of it; DHS was trying to figure out the election side of it. We are past that, we really committed to working together, we have built partnerships, we have established trust and we are really getting to that point of understanding what they need from us and we are reacting accordingly. So I have great confidence that if we did see something, that I would know exactly who to go to in each State to share that information.

We will not be in a position like we were in 2016, when, frankly, we were in kind of uncharted territory, for us at the time, at least.

Ms. BARRAGÁN. So are you suggesting that the then-under secretary didn't know who to call at these—in these States, to let them know—

Under Secretary KREBS. There was no election infrastructure subsector. So these relationships were not established at the time. So my predecessor, who I have spoken with about this, they—what they did was follow a traditional incident response protocol. They notified the State or the asset owner, which may have been a county or may have been a private-sector owner-operator, and that is the playbook.

Going through the process now, we understand that this is a unique community, this is a unique subsector, and what works in other sectors doesn't work here, and we have changed our protocols accordingly.

Ms. BARRAGÁN. Is DHS in a position to detect if there is such meddling happening in all of the 50 States? In other words, does DHS have any visibility into whether relevant State systems are being targeted?

Under Secretary KREBS. So since, frankly, February of this year, we have quadrupled our insight into State activities. We have an intrusion detection system that is called Albert, it is similar to a system the Federal Government uses, that we have deployed out. Now, I mentioned 21 States earlier, in part, those 21 States, we saw that activity because of the deployed Albert sensors at the time.

Like I mentioned, we have quadrupled our insights since just February of this year. By the mid-terms of—by November of this year, we will have almost every State covered down on and we have significant coverage across counties in other jurisdictions.

Ms. BARRAGÁN. OK. My understanding is that there is no Nationally-mandated security requirements for election technology vendors nor are they subject to a consistent set of breach notification laws. How would you characterize DHS's relationship with election-related vendors?

Under Secretary KREBS. So, we—there are actually a complementary group called the Sector Coordinating Council. So, on the Government Coordinating Council you have State and local election officials and then on the Sector Coordinating Council side, we have vendors will all the major technology providers to elections.

Frankly, we took up, kind-of, an incremental approach. We started building strong relationships with the State partners and local partners and we are moving—we have the Sector Coordinating Council established and the relationships are growing. They are not, frankly, probably where they need to be, but they are getting there.

Ms. BARRAGÁN. My last question to you sir, is, we know that the President doesn't believe in the meddling and you have already indicated you believe the intelligence reports. What does it do to morale, to the people under you to know that their commander, the top guy, doesn't even believe that there was any meddling when that is what you guys are doing? Your mission is to go out and stop

it from happening and preventing, you know, them to interfere in our democracy. What does that do to the people under you?

Under Secretary KREBS. I think generally speaking, the morale on my team is really high right now. I think the ability to work with folks with Secretary Gorbea—the way I see it, a high functioning organization.

Ms. BARRAGÁN. So, you don't see an impact at all from the President's speak about this to your team?

Under Secretary KREBS. I am just saying in general, the morale of my team is very high.

Ms. BARRAGÁN. Great, thank you.

Chairman MCCAUL. The gentlelady yields. The gentleman from Massachusetts, Mr. Keating, is recognized.

Mr. KEATING. Thank you, Mr. Chairman. I would like to thank you for being here. Just a question since I had a conflicting hearing. But what is the attitude—range of attitude among local and State officials when you are saying, we are here to give you some help? Do some of them say, don't worry I have it covered, I am confident our system is fine? Is that something you hear?

Under Secretary KREBS. Every State is a different experience.

Mr. KEATING. No, but have you heard that? That is what I asked.

Under Secretary KREBS. I have heard some States say, we are resourced. I have been told rather that some States have said, we have the resources and the capabilities—

Mr. KEATING. Are you just waiting—have you reached out to all the State and local officials?

Under Secretary KREBS. We have engaged every single State.

Mr. KEATING. OK. So, you have heard back from those officials or you?

Under Secretary KREBS. Yes, sir.

Mr. KEATING. So, some of them just feel confident, no problem, got it covered?

Under Secretary KREBS. Every State is working with DHS in some capacity.

Mr. KEATING. Well, I know that. I just asked what your experience was. I mean, it is not a tough question. It is just—are you getting that feedback, don't worry, I am confident, I have got it covered, from those officials?

Under Secretary KREBS. Yes, sir. I think some States feel that they have—they are adequately resources or adequately supported. Others, like insurance policies, and even though they may have things covered, they will still take some of our—

Mr. KEATING. Do you think that we are going to be attacked in 4 months by Russia?

Under Secretary KREBS. Sir, I don't have any information or evidence to suggest they are going to attack us, but we don't need that.

Mr. KEATING. Do you share information with our intelligence officials, then?

Under Secretary KREBS. They share with me, yes, sir. I am not a collector.

Mr. KEATING. They believe we are going to be attacked. So, you don't believe—opinions.

Under Secretary KREBS. I don't think I have seen that assessment that they are going to attack our election. That the—Secretary Gorbea—

Mr. KEATING. You haven't heard that from our intelligence officials? U.S. intelligence official, you haven't heard that one?

Under Secretary KREBS. I have—you know, maybe I need to go back and review, but.

Mr. KEATING. Yes, I think so. I think—

Under Secretary KREBS. Sir, I think what they have said is that—

Mr. KEATING. I think our intelligence officials are saying they are going to do it again.

Under Secretary KREBS. I think that they have.

Mr. KEATING. Meaning Russia.

Under Secretary KREBS. Yes, sir. Russia, I think they—Russia is engaging in information operations whether it is focused on elections or not.

Mr. KEATING. Well, our intelligence—maybe I am wrong? But intelligence is saying—

Under Secretary KREBS. No, I am—sir, I am not suggesting.

Mr. KEATING. They are going to do it again. You don't believe they are going to do it again?

Under Secretary KREBS. I wouldn't put—

Mr. KEATING. You don't agree with our intelligence officials?

Under Secretary KREBS. I wouldn't put anything past the Russians. I am not disagreeing with any intelligence. I am just—what I am saying is.

Mr. KEATING. I am just saying, don't you agree with our intelligence—the people that are saying that?

Under Secretary KREBS. Yes sir, I agree—

Mr. KEATING. Wow. That was—

Under Secretary KREBS. With our intelligence community.

Mr. KEATING. Sorry about that, but. Are we sufficiently ready for this attack? What kind of guarantee can you give us that we are up to the task?

Under Secretary KREBS. I have confidence in the resilience of the system. I have, I think, some of the controlling measures that we have in place, whether it is provisional ballots as we discussed or some of the other compensating controls. We think, you know, is it 100 percent—

Mr. KEATING. Can you guarantee?

Under Secretary KREBS. Of course not.

Mr. KEATING. No. And it is likely that there could be some difficulty. It is in the realm of possibility, correct?

Under Secretary KREBS. Sir, I, you now, I am paid to be paranoid. I plan for bad days and that is what we are working toward.

Mr. KEATING. Yes. Well, have you reached out, as a rule, and communicated the fact that it is likely we are going to be attacked now that you know that, and will—in fact, will be attacked? No. 2, that despite the great efforts of mitigating this that can't cover that, have you reached out to all of our officials and said, we believe, strongly, you should move to paper ballots?

Under Secretary KREBS. It is a baseline recommendation of the Department, working with the GCC and others that—yes, paper trails, verifiable, auditable paper trails are a best practice, period.

Mr. KEATING. Yes. Secretary Gorbea, what are you—what are your colleagues, Nation-wide, what are you hearing back? I mean, to me this is a strong statement that you come from. Despite our efforts, you know, our best efforts to try and mitigate this, that there should be paper ballots? That is what we should be doing, frankly.

Ms. GORBEA. I wholeheartedly agree and I give a lot of credit to Congressman Langevin for when he was the Secretary of State. He started us on this paper ballot process with optical scan readers and when I came into office those—that equipment was outdated and we replaced it with similar because there should always be something that you can touch and feel that you and I can look at and say, this is how the voter wanted to—

Mr. KEATING. Particularly provisional ballot because if they do get in the infrastructure and they can manipulate data, those provisional ballots are going to be critical.

Ms. GORBEA. That is right. But that is where looking at the various systems and rules around provisional ballots are really important because in Rhode Island, those provision ballots are reviewed by election officials—

Mr. KEATING. Is our government, the U.S. Government, the Federal Government, communicated to all election officials sufficiently, in your opinion, that there will be an attack that their efforts to mitigate it, but no guarantees there that they can be successful; you should move to paper ballots. Has it been that strong a message or is just the recommendation?

Ms. GORBEA. I think we are all in this space, very concerned about making sure that we mitigate the risk. We don't need, necessarily, the Federal Government to tell us this because we see it everywhere. So, I think all States are taking measures.

Mr. KEATING. How many States are moving to paper ballots? It is 4 months away.

Ms. GORBEA. I don't have the answer to that, but the National Association of Secretaries of State might be able to provide that.

Mr. KEATING. Do you know, Under Secretary Krebs?

Under Secretary KREBS. Sir, I know that 5 States, right now, are exclusively on non-paper ballot systems. Of those 5, 4 are in the RFP process. One is, you know, waiting for money, frankly.

Mr. KEATING. So, it is pretty prevalent that there is going to be paper ballots? That is reassuring.

KREBS: It—so, I think on the balance there are paper ballots, but there are still systems out there that do not have paper ballots.

Mr. KEATING. Percentage-wise, again?

Under Secretary KREBS. Off the top of my head, I don't have percentages.

Mr. KEATING. I would suggest that is something we should know. That would be—

Under Secretary KREBS. So, happy to.

Mr. KEATING. That you could do that.

Under Secretary KREBS. Yes, sir, happy to circle back with—and work with the Election Assistance Commission—

Mr. KEATING. That would be helpful.

Under Secretary KREBS. And the secretaries——

Mr. KEATING. I realize your limitations. I appreciate your testimony and your good work. As a last comment, dealing with the Russians, our intelligence said they are doing it again. We have to have deterrents, as well as a rope-a-dope approach, where we are just doing our best to mitigate it, and I hope that is done. I know it is not in your specific purview. It is certainly not yours at the State level, but in the interim, I think we should give the strongest message possible for paper ballots. That will deter them in the actual infrastructure apparatus attempts to get into our system. On a larger scale, I believe very strongly that the sanctions and the deterrents that we have at the upper levels are critical. So thank you for your work. I yield back.

Chairman MCCAUL. The gentleman yields. The gentlelady from Texas, Ms. Jackson Lee, is recognized.

Ms. JACKSON LEE. Let me thank the Chairman and Ranking Member for holding this hearing, and to the witnesses, let me thank you, as well. Committee business in judiciary proceeding on issues that dealt with the 2016 election delayed me. But this is an important hearing, and I want to follow the line of reasoning of my colleague, Mr. Keating, and maybe in a different perspective.

To both of you, let me thank you for the service that you give. But I believe that this will be a Federal election in a large way. The Congress will be up for reelection, the House in totality, the Senate partially. So this is a Federal election, and I have the greatest respect for State officers, and they are our collaborators. But I would say to the Secretary that it is the responsibility of the Federal Government to at least provide the structure and the walls of security upon which you can work within, or even add to by your own expertise.

With that in mind, I frankly believe that this Government has not been effective in recognizing the larger picture, and that is the enormous involvement and invasion that Russia perpetrated in 2016, and in elections before that, where we probably did not have all of the analysis. I do not believe that we are solidly in control, and facing what is a potential of invasion, interference, and altering and skewing of the election by the Russians, and maybe some others. I don't believe, in particular, that the commander-in-chief has been particularly effective in acknowledging that invasion in 2016, and I would hope in his meeting that I certainly have concern with, with Vladimir Putin, that that will be No. 1 in his agenda.

Secretary Krebs, do you know whether the President will be discussing election fraud, election challenges, in his meeting with the head of Russia?

Under Secretary KREBS. Yes, ma'am, that is my understanding.

Ms. JACKSON LEE. Have you given him or the Secretary of Homeland Security—I don't know if she is there, but the State Department, those are all diplomats. Have you given him a matrix, a list of questions or information to the White House that he will be well-informed in his questioning?

Under Secretary KREBS. Ma'am, I personally have not, and I would need to get back to you on whether the Secretary——

Ms. JACKSON LEE. But you think it would be important that those questions be raised?

Under Secretary KREBS. I think that that is a useful conversation, yes, ma'am, just a——

Ms. JACKSON LEE. I hope more than useful. Let me——

Under Secretary KREBS. Stern warning, yes ma'am.

Ms. JACKSON LEE. Earlier this year, I introduced H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act, which passed the House earlier this year with the help of this committee and the Chairman and Ranking Member. The bill requires the Secretary of Homeland Security to submit a report on the policies and procedures developed for coordinating cyber availability disclosures. The report will include an annex with information on instances in which cybersecurity vulnerability, disclosure policies, and procedures were used to disclose details on identified weaknesses in computing sciences or digital services at risk. The report will provide information on the degree to which the information provided by DHS was used by industry and other stakeholders in a closed setting.

The reason I worked on this bill before the full House for consideration is a problem often referred to as “zero-day events.” Zero-day event describes the situation that network security professionals may find themselves when a previously unknown error or flaw in computing code is exploited by cyber criminals, or terrorists, or someone who wants to undermine our elections. That is the level that I think we may be at, at some point in our election.

So, Mr. Secretary, I ask you, do you, in fact, have the kind of infrastructure at DHS that can be prepared for catastrophic events dealing with the Nation’s democracy, these elections? DHS employees stand on the front lines of Federal Government efforts to defend our Nation’s critical infrastructure from natural disasters, terrorism, adversarial threats, technological risks such as those caused by cyber threats.

So my concern would be elections that I hope are classified as critical infrastructure. Are you confident that you have a team that, if the secretary from Rhode Island reaches out, even with her good works, to the Federal Government, where are we in protecting election, detecting Russian invasion and altering our election system?

Mr. KREBS. So generally speaking, I think we have a team that is elastic, in that we can focus on a number of different infrastructure sectors, and when an acute need arises, we can surge into a specific sector like election infrastructure. So if I got that call from Secretary Gorbea, and she needed a fly-in team of “X” number of people, we could deliver that.

With more, though, I can, of course, do more. So we are taking a look at what the threat picture looks like, what our ability to manage risk across the country is, and the demand signal from our stakeholders. All of our engagements are voluntary in this space, so I have to have a requirement set. I have to have a demand signal. If Secretary Gorbea needs something, and if I get 49 other secretaries that say they need something, that compounds into a very clear demand——

Ms. JACKSON LEE. So do we need to write legislation to give you requirements of indicia that says, this is when you shoot into a State that is impacted by what they think is a cyber threat in their elections, and you need to dispatch. Are you voluntarily sending staff there? Or do you have legislative authority?

Under Secretary KREBS. I think it is a—I have legislative authority to send folks on instant response capabilities. That was already been provided.

Ms. JACKSON LEE. And resources? And resources?

Under Secretary KREBS. So it depends on the level of the incident. You know, we don't have 1,000 people sitting on a bench waiting for a phone call. We have folks that are providing incident response capabilities. They are providing hunt capabilities, risk and vulnerability assessments. It is based—like I said, elasticity is critical here, because folks can do something on Monday, and they do something different on Tuesday, and we will deal with surge.

Ms. JACKSON LEE. Well, Mr. Secretary, it was humorous to say 1,000 people on the bench. Some of us are very much into sports, and we would like to have 1,000 so we could substitute out those who are not working. But the point is it may be 1,000—you know, this is a big Nation, 300 million-plus, and it may be 1,000 incidents in the middle of a high-profile election.

I consider the Federal elections certainly are the highest profile, although State elections, Governors, State legislators and others certainly are part of the democratic infrastructure.

What I am saying is, with all seriousness, that I believe that you should be prepared in this infrastructure scheme, and there are many others. I could be talking about the electric grid and others. I don't have the time to do so. But I want to focus, because I don't believe that the administration—and you are in there as part of it. I am not saying your direct office—has given this the attention and the sensitivity and seriousness that I, frankly, believe puts you in the seat, along with the Secretary of Homeland Security to get those 1,000 people on the bench, and if they are needed from sea to signing she—signing she—sea, that we are able to protect the election of the voters of the American people. That is what I am trying to hear from you.

Secretary KREB. Yes, ma'am, I understand your concern.

I will tell you this much, and hopefully the experience is validated by Secretary Gorbea, but I spend 40 to 50 percent of my time right now, almost exclusively on elections. There is no way I could take this any more seriously than I do and my team sees that. We have capabilities across this organization that are able to surge in to this space.

So when we think about mid-terms, when we think about November—there are protective security advisors distributed across this country, 130 or 140 of them. I have got cybersecurity advisors distributed across this country, on any given day they are working across the 16 sectors. In November they will be focused on election infrastructure; that is just that group. I have other folks in the District of Columbia that will be focusing on elections, so we are able to surge in to the space.

That said, I can always do more—with more I can always do more. So we are continuing to work with our stakeholders to un-

derstand what it is they need from us, and then that refines our resource requirements.

Ms. JACKSON LEE. I thank you, Mr. Chairman, I am yielding back. I would ask the Secretary to think of an SOS number that could be given out as we move toward elections. If I am out in a field and somebody says I am totally collapsed and my local people can't find out why they are collapsed or what is going on, whether we should move to provisional, would be helpful to have that one SOS number.

Secretary KREB. Yes, ma'am.

Ms. JACKSON LEE. With that, Mr. Secretary, will you take that under advisement, be able to say yes?

Secretary KREB. Yes, ma'am.

Ms. JACKSON LEE. All right, thank you very much. I yield back, thank you.

Chairman MCCAUL. Gentlelady yields, I am going to think—Ranking Member, I mean, closing. I would like to thank our witnesses for being here today, I just wanted to conclude with a short personal experience.

Over 20 years ago, I was a Federal prosecutor, Justice, and I prosecuted a guy named Johnny Chung who lead us to the Director of Chinese Intelligence, who was acting on behalf of China Aerospace because he liked then-President Clinton's position on technology transfers. He put money in to Johnny Chung's Hong Kong bank account to put in to the Presidential election.

So my point is, is that this is nothing new, foreign adversaries influencing our elections and Presidential elections. I think it has been going on for quite some time. I think now, they have found a new tool to use and manipulate to do that, and that is the internet and cyber space.

So with that I want to thank both of you for your strong leadership on this issue. We take this very seriously in the Congress on both sides of the aisle as we enter into the mid-term elections. If there's anything this committee can do to help you in your efforts, please let us know.

Members may have additional questions they may submit in writing, and pursuant to Committee rule VII(D) the hearing record will stay open for 10 days.

Without objection, committee stands adjourned.

[Whereupon, at 12:38 p.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM HONORABLE JOHN KATKO FOR CHRISTOPHER C. KREBS

Question 1. Obviously, cybersecurity is a hot topic that many Government agencies have a piece of. But I think the one thing we learned after 9/11 was the potential damage that can be done when Government resources and intelligence are segmented and stove-piped. Can you speak to the importance of clarifying the roles and responsibilities of your directorate not only at the Department, but across the Federal Government to your ability to move this Nation toward more robust cybersecurity policies and practices?

Answer. The Department has been provided clear roles and responsibilities authorized by several statutes passed in 2014 and 2015, and are codified primarily in Title II of the Homeland Security Act (the Act); the Cybersecurity Information Sharing Act of 2015 (CISA); and subchapter II, chapter 35 of title 44, U.S. Code, as created by the Federal Information Security Modernization Act of 2014 (FISMA). These functions are also supported by several important Executive branch documents, including Presidential Policy Directives 21 and 41. These actions have furthered DHS's cybersecurity mission since its inception and codified interagency roles and responsibilities. Specifically, the Department placed the National Cybersecurity and Communications Integration Center (NCCIC) within the DHS National Protection and Programs Directorate to serve as the round-the-clock operational center that executes the Department's cybersecurity and communications mission. The NCCIC is a lead civilian interface for sharing cyber threat information with the Government that is uniquely positioned as a sharing hub to integrate information from multiple sources, and use it to provide Government agencies and the private sector with actionable information to recognize, prevent, and mitigate harm from cyber attacks. As such, the NCCIC facilitates multi-directional information sharing between the Federal Government and the private sector.

It is critical that Congress pass the Cybersecurity and Infrastructure Security Agency Act in order to reinforce NPPD's role as currently performed. This law will establish a cybersecurity agency at the Department of Homeland Security to further National efforts to enhance the security and resilience of U.S. cyber and physical critical infrastructure.

Question 2. Among the challenges that we face in cybersecurity is the pace at which our adversaries adapt their tactics, techniques, and procedures as we harden our own systems and networks. Are there any particular methods of attack or vectors of intrusion that DHS is focusing on during the upcoming election cycle?

Answer. Many of the methods of attack and vectors of intrusion that DHS sees can be avoided through implementation of basic cyber hygiene mitigation efforts. As a result of malicious actors exploiting unpatched software, conducting phishing campaigns, and leveraging common vulnerabilities to pursue attacks against critical infrastructure organizations, we emphasize with the election community the myriad of attack vectors in order to increase the defense and resiliency of the election infrastructure.

Question 3. Is NPPD being given access to all the necessary access to and information from the intelligence and law enforcement community to ensure you are in a position to accurately measure the risks to our election system? Can you say the same thing for the other sectors that have been designated critical infrastructure?

Answer. To most effectively share information with all of our partners—not just those with security clearances—DHS works with the intelligence community to declassify relevant intelligence or provide tearlines as much as possible. While DHS prioritizes declassifying information to the extent possible, DHS also provides Classified information to cleared stakeholders, as appropriate.

Although more work is needed, DHS's goal is to ensure that law enforcement and the intelligence community are sharing all relevant information and that it is in a

format that can be widely disseminated to critical infrastructure partners. This work is a vital part of our information-sharing efforts.

QUESTIONS FROM HONORABLE JOHN RATCLIFFE FOR CHRISTOPHER C. KREBS

Question 1. The Election System is just one part of the critical infrastructure security responsibilities that DHS has. Is there a need for each of these sectors to create their own cybersecurity information centers like the NCCIC or would such a splintering of Federal resources potentially harm the security of Nation?

Answer. To break down information stovepipes and ensure cross-sector approaches to protecting our Nation, the Department's specific cybersecurity authorities executed through NPPD—including authorities related to sharing, analyzing, and coordinating actionable information related to cybersecurity risks and incidents; protecting Federal information systems; and responding to cybersecurity incidents—enable NPPD to engage with Federal and non-Federal entities (i.e. all stakeholders—public, private, and international) and across and beyond all critical infrastructure sectors to collaboratively improve cybersecurity practices and protect Federal and non-Federal entities from cyber risks. While Sector-Specific Agencies have specific roles with respect to working with their stakeholders, DHS has the lead for understanding and providing cross-sector information, analysis, and protective measures to all sectors. If agencies work within stovepipes with their stakeholders, then other sectors are not afforded the critical information related to new attack vectors and identified vulnerabilities. Congress has taken specific action to overcome this challenge and clarify DHS's role to prevent stovepipes across critical infrastructure sectors. The Homeland Security Act was amended in 2014 and 2015 to codify the role of the Department's National Cybersecurity and Communications Integration Center (NCCIC) as the Federal-civilian interface for sharing information regarding cybersecurity risks and incidents and authorize the NCCIC to provide cybersecurity-related technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities. In a similar fashion, the Cybersecurity Act of 2015 also establishes the NCCIC as the Federal Government's central hub for sharing cyber threat indicators between the private sector and the Federal Government and requires the Department to establish the Federal Government's capability and process for sharing cyber threat indicators with both Federal and non-Federal entities. DHS operates a central hub for information exchange, technical expertise, operational partnerships, and systems-focused cybersecurity capabilities through the National Cybersecurity and Communications Integration Center.

Cross-sector coordination of the Federal Government's cybersecurity efforts is critical to our Nation's National security, economic security, public health, and safety. Information regarding situational awareness, vulnerability, and incidents must be shared as quickly as our adversaries move in cyber space.

Question 2. Can you speak to the importance of clarifying the roles and responsibilities of your directorate, not only at the Department, but across the Federal Government, for your ability to move this Nation towards more robust cybersecurity policies and practices?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR CHRISTOPHER C. KREBS

Question 1a. On April 24, Assistant Secretary Jeanette Manfra testified before the Senate Homeland Security and Government Affairs Committee that the surge in risk and vulnerability assessments for elections infrastructure created "a significant backlog in other critical infrastructure sectors and Federal agencies" waiting for similar assessments. The President's 2019 budget did not request an increase in resources sufficient to overcome this backlog.

Are more resources necessary to support the increased requests from State and local governments without delaying other assessments?

Question 1b. What is the current RVA backlog? What is the prognosis for that backlog over the next calendar year?

Answer. Currently, about 28 critical infrastructure entities and Federal agencies have Risk and Vulnerability Assessments (RVAs) that have been scheduled at a later date due to the critical, time-sensitive prioritization of election-related RVAs. For the RVAs unrelated to elections, the wait time is at least 100 days for entities prioritized at the top of the list and indefinite for those at a lower priority. Federal agencies and entities in the chemical, emergency services, energy, financial services, Government facilities, transportation, water and wastewater, food and agriculture, defense industrial base, and information technology sectors have been impacted. The RVA queue is dynamic and reprioritized as part of a quarterly scheduling routine.

With current resource capacity, the waiting list for RVAs cannot be eliminated. Federal agencies and critical infrastructure entities are regularly added to the schedule. To date 98 RVAs have been completed, of which 29 were Election-based RVAs. In fiscal year 2019, NPPD plans to conduct 90 RVAs, of which 30 will be performed on Federal High-Value Assets. The remaining 60 RVAs will be determined in accordance with our prioritization process and methodology.

Question 2a. Based on the RVAs that DHS has carried out for State and local election officials, do most States and localities have the resources required to sufficiently mitigate their cybersecurity vulnerabilities (including equipment, staffing, training, and other components that factor into security)?

Question 2b. If not, how big is the shortfall?

Answer. Through the fiscal year Department of Homeland Security (DHS) Appropriations Act and a reprogramming request, DHS was provided with approximately \$26 million to support election infrastructure security activities. These additional funds have been covering a number of efforts to enhance the security and resilience of election infrastructure.

NPPD provides assistance to State and local election officials to help them determine where vulnerabilities may exist. However, decisions about how to resource election infrastructure security enhancements are made solely by those officials. Through the Election Assistance Commission, Congress recently made \$380 million in funding available to State and local election officials to improve cybersecurity of Federal elections. The money is intended to provide an additional infusion of funding for new resources and personnel to improve Federal elections. Congressional support of funding for these activities is appreciated.

Question 3. In the guidance NPPD issued to election officials on how to spend security funding, NPPD emphasizes the importance of deploying auditable voting systems.

How important is it that States have auditable paper trails and conduct post-election audits to verify the digital tallies of election results?

Answer. As noted in the prior question, through the Election Assistance Commission, Congress recently made \$380 million in funding available to State and local election officials to improve the cybersecurity of Federal elections which will provide an additional infusion of funding for new resources and personnel to improve Federal elections.

Deploying auditable voting systems is critical to the resilience of the process and is being prioritized by many States. With the continued move to auditable systems, post-election auditing has become a common practice for many election jurisdictions. However, for many offices, the post-election audit process is time-consuming and costly. Improving the overall efficiency and effectiveness of post-election audits is a quick way to improve the overall integrity of the process. Simple steps like hiring more temporary staff to organize and run the post-election audit is an effective way to lessen the burden on already over-worked and under-staffed election offices while improving the overall resilience of the process.

Question 4. Much of DHS's mission requires close coordination with other agencies, especially with respect to cybersecurity.

How has the Department's ability to synchronize its cyber mission with other agencies been affected by the elimination of the Cybersecurity Coordinator position and the recent high rate of turnover at the National Security Council?

Answer. Changes made within the National Security Council staff related to the Cybersecurity Coordinator have had no impact on DHS's ability to execute its mission. The President has provided clear direction to DHS and other National security agencies to execute our authorities and responsibilities. DHS and our interagency partners continue to coordinate regularly, through the National Security Council staff, on policy matters and our operational centers.